UNCLASSIFIED

IBM z/OS TSS Security Technical Implementation Guide

Version: 8

Release: 11

25 Oct 2023

XSL Release 1/25/2022 Sort by: STIGID
Description: This Security Technical Implementation Guide is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements are derived from the National Institute of Standards and Technology (NIST) 800-53 and related documents. Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil.

Group ID (Vulid): V-223871
Group Title: SRG-OS-000066-GPOS-00034
Rule ID: SV-223871r877712_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-CE-000010
Rule Title: All IBM z/OS digital certificates in use must have a valid path to a trusted Certification Authority (CA).
Legacy ID: SV-107553
Legacy ID: V-98449

Vulnerability Discussion: Without path validation, an informed trust decision by the relying party cannot be made when presented with any certificate not already explicitly trusted.

A trust anchor is an authoritative entity represented via a public key and associated data. It is used in the context of public key infrastructures, X.509 digital certificates, and DNSSEC.

When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor; it can be, for example, a CA. A certification path starts with the subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted CA.

This requirement verifies that a certification path to an accepted trust anchor is used for certificate validation and that the path includes status information. Path validation is necessary for a relying party to make an informed trust decision when presented with any certificate not already explicitly trusted. Status information for certification paths includes certificate revocation lists or online certificate status protocol responses. Validation of the certificate status information is out of scope for this requirement.

Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000403-GPOS-00182

Check Content:
Execute the CA-TSS SAFCRRPT using the following as SYSIN input:
RECORDID(-) DETAIL TRUST FIELDS(ISSUER SUBJECT ACTIVE EXPIRE TRUST)

If no certificate information is found, this is not a finding.

NOTE: Certificates are only valid when their Status is TRUST. Therefore, you may ignore certificates with the NOTRUST status during the following check.

If the digital certificate information indicates that the issuer's distinguished name leads to one of the following this is not a finding:
a) A DoD PKI Root Certification Authority

b) An External Root Certification Authority (ECA)
c) An approved External Partner PKI's Root Certification Authority

The DoD Cyber Exchange website contains information as to which certificates may be acceptable (https://public.cyber.mil/pki-pke/interoperability/ or https://cyber.mil/pki-pke/interoperability/).

Examples of an acceptable DoD CA are:
DoD PKI Class 3 Root CA
DoD PKI Med Root CA

Fix Text: Remove or replace certificates where the issuer's distinguished name does not lead to a DoD PKI Root Certification Authority; External Root Certification Authority (ECA); or an approved External Partner PKI's Root Certification Authority.

The DoD Cyber Exchange website contains information as to which certificates may be acceptable (https://public.cyber.mil/pki-pke/interoperability/ or https://cyber.mil/pki-pke/interoperability/).

CCI: CCI-000185

CCI: CCI-002470

Group ID (Vulid): V-223872
Group Title: SRG-OS-000066-GPOS-00034
Rule ID: SV-223872r877713_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-CE-000020
Rule Title: Expired IBM z/OS digital certificates must not be used.
Legacy ID: SV-107555
Legacy ID: V-98451

Vulnerability Discussion: Without path validation, an informed trust decision by the relying party cannot be made when presented with any certificate not already explicitly trusted.

A trust anchor is an authoritative entity represented via a public key and associated data. It is used in the context of public key infrastructures, X.509 digital certificates, and DNSSEC.

When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor; it can be, for example, a Certification Authority (CA). A certification path starts with the subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted CA.

This requirement verifies that a certification path to an accepted trust anchor is used for certificate validation and that the path includes status information. Path validation is necessary for a relying party to make an informed trust decision when presented with any certificate not already explicitly trusted. Status information for certification paths includes certificate revocation lists or online certificate status protocol responses. Validation of the certificate status information is out of scope for this requirement.

Check Content:
Execute the CA-TSS SAFCRRPT using the following as SYSIN input:
RECORDID(-) DETAIL FIELDS(ISSUER SUBJECT ACTIVE EXPIRE TRUST)

If no certificate information is found, this is not a finding.

NOTE: Certificates are only valid when their Status is TRUST. Therefore, you may ignore certificates with the NOTRUST status during the following checks.

Check the expiration for each certificate with a status of TRUST.

If the expiration date has passed, this is a finding.

Fix Text: If the certificate is a user or device certificate with a status of TRUST, follow procedures to obtain a new certificate or re-key certificate. If it is an expired CA certificate remove it.

CCI: CCI-000185

Group ID (Vulid): V-223873
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223873r877714_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-CE-000030
Rule Title: IBM z/OS must have Certificate Name Filtering implemented with appropriate authorization and documentation.
Legacy ID: V-98453
Legacy ID: SV-107557

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to

have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
If certificate name filtering is in use, the ISSM should document each active filter rule and have written approval to use the rule.

Issue the following TSS command to list any certificate name filters defined to TSS:

TSS LIST(SDT) CERTMAP(ALL)

If there is nothing to list, this is not a finding.

NOTE: Certificate name filters are only valid when their Status is TRUST. Therefore, you may ignore filters with the NOTRUST status.

If certificate name filters are defined and they have a Status of TRUST, certificate name filtering is in use.

If certificate name filtering is in use and filtering rules have been documented and approved by the ISSM, this is not a finding.

If certificate name filtering is in use and filtering rules have not been documented and approved by the ISSM, this is a finding.

Fix Text: Ensure any certificate name filtering rules in use are documented and approved by the ISSM.

CCI: CCI-000764

Group ID (Vulid): V-223874
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223874r877715_rule
Severity: CAT I

Rule Version (STIG-ID): TSS0-ES-000010
Rule Title: CA-TSS Security control ACIDs must be limited to the administrative authorities authorized and that require these privileges to perform their job duties.
Legacy ID: SV-107559
Legacy ID: V-98455

Vulnerability Discussion: The use of security policy filters provides protection for the confidentiality of data by restricting the flow of data. A crucial part of any flow control solution is the ability to configure policy filters. This allows the operating system to enforce multiple and different security policies. Policy filters serve to enact and enforce the organizational policy as it pertains to controlling data flow.

Check Content:
From the ISPF Command Shell enter:

TSS LIST(ACIDS) DATA(ADMIN, BASIC)

If any ACIDs other than TYPE=CENTRAL (SCA/MSCA) has the following administrative authority, this is a finding.

FACILITIES(ALL)
PROGRAM(ALL)
PROGRAM(OWN)
RESOURCE(ALL)
ROSRES(ALL)
VOLUME(ALL)
VOLUME(OWN)

MISC1(ALL)
MISC1(LCF)
MISC1(LTIME)
MISC1(RDT)
MISC1(USER)

MISC2(ALL)
MISC2(DLF)
MISC2(NDT)
MISC2(SMS)

MISC4(ALL)

MISC8(ALL)
MISC8(LISTAPLU)
MISC8(LISTRDT)

MISC8(LISTSDT)
MISC8(LISTSTC)
MISC8(MCS)

MISC9(ALL)
MISC9(BYPASS)
MISC9(CONSOLE)
MISC9(GLOBAL)
MISC9(MASTFAC)
MISC9(MODE)
MISC9(STC)
MISC9(TRACE)

Fix Text: Review all security administrator ACIDs. Evaluate the impact of limiting the amount of excessive administrative authorities. Develop a plan of action and implement the changes.

The following are examples for other types (DCA, VCA, ZCA, LSCA) that require administrative authorities: (note: these are examples and does not mean everyone should have all of these levels).

data set(ALL)ACC(ALL)
data set(XAUTH,OWN,REPORT,AUDIT,INFO)ACC(ALL)
OTRAN(ALL)ACC(ALL)
ACID(ALL)
ACID(INFO,MAINTAIN)
MISC1(INSTDATA,SUSPEND,TSSSIM,NOATS)
MISC2(TSO,TARGET)
MISC8(PWMAINT,REMASUSP)
MISC9(GENERIC)
FACILITY(BATCH, TSO, ROSCOE, CICS, xxxx)

Where "xxxx" is a facility the application security team grants access into for their application users. This must not be STC, CA1, DFHSM, or other domain level mastfac/facility. This is only for those "onlines" that users truly log in to for access to their applications/data such as TSO, CICS regions, IDMS, ROSCOE, FTP, etc.

TSS ADMIN(acid)RESOURCE(REPORT,INFO,AUDIT) can be allowed and is required to run TSSUTIL reports.

Note: "RESOURCE" can specify a more specific Resource Class, such as "OTRAN", "data set", "IDMSGON", "PROGRAM" for non SCA/MSCA type of accounts. These administrators will not have "RESOURCE" specified in administrative authority.

Note: "ALL" will display as "*ALL*" but also means approved for any single administrative authority under that specific item.

CCI: CCI-000213

Group ID (Vulid): V-223875
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223875r877716_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000020
Rule Title: The number of CA-TSS ACIDs possessing the tape Bypass Label Processing (BLP) privilege must be limited.
Legacy ID: SV-107561
Legacy ID: V-98457

Vulnerability Discussion: The use of security policy filters provides protection for the confidentiality of data by restricting the flow of data. A crucial part of any flow control solution is the ability to configure policy filters. This allows the operating system to enforce multiple and different security policies. Policy filters serve to enact and enforce the organizational policy as it pertains to controlling data flow.

Check Content:
From the ISPF Command Shell enter:
TSS LIST(ACIDS) DATA(BASIC)

If only authorized personnel have BLP access and documentation for access is on file with the ISSO, this is not a finding.

Fix Text: Review all ACIDs with the BLP attribute. Evaluate the impact of removing BLP access from unauthorized personnel. Develop a plan of action and remove BLP access from unauthorized ACIDs.

CCI: CCI-000213

Group ID (Vulid): V-223876
Group Title: SRG-OS-000001-GPOS-00001
Rule ID: SV-223876r877717_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000030
Rule Title: CA-TSS MODE Control Option must be set to FAIL.
Legacy ID: SV-107563
Legacy ID: V-98459

Vulnerability Discussion: Enterprise environments make account management challenging and complex. A manual process for account management functions adds the risk of a potential oversight or other errors.

A comprehensive account management process that includes automation helps to ensure accounts designated as requiring attention are consistently and promptly addressed. Examples include, but are not limited to, using automation to take action on multiple accounts designated as inactive, suspended, or terminated, or by disabling accounts located in non-centralized account stores such as multiple servers. This requirement applies to all account types, including individual/user, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.

The automated mechanisms may reside within the operating system itself or may be offered by other infrastructure providing automated account management capabilities. Automated mechanisms may be composed of differing technologies that, when placed together, contain an overall automated mechanism supporting an organization's automated account management requirements.

Account management functions include: assigning group or role membership; identifying account type; specifying user access authorizations (i.e., privileges); account removal, update, or termination; and administrative alerts. The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using automated telephonic notification to report atypical system account usage.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the global MODE Control Option value is set to "FAIL", this is not a finding.

If the global MODE Control Option value is not set to "FAIL", this is a finding.

Additional analysis may be required under the following conditions:
Mode(IMPL) is allowed while a system is in implementation with a documented process that includes an implementation completion date.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to set the MODE control option to (FAIL) and proceed with the change.

CCI: CCI-000015

Group ID (Vulid): V-223877
Group Title: SRG-OS-000021-GPOS-00005
Rule ID: SV-223877r877718_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000040
Rule Title: The CA-TSS NPWRTHRESH Control Option must be properly set.
Legacy ID: SV-107565
Legacy ID: V-98461

Vulnerability Discussion: By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the NPWRTHRESH Control Option value is not set to NPWRTHRESH(02), this is a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting as specified following and proceed with the change.

NPWRTHRESH(02)

CCI: CCI-000044

Group ID (Vulid): V-223878
Group Title: SRG-OS-000021-GPOS-00005
Rule ID: SV-223878r877719_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000050
Rule Title: The CA-TSS NPPTHRESH Control Option must be properly set.
Legacy ID: V-98463
Legacy ID: SV-107567

Vulnerability Discussion: By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the NPPTHRESH Control Option value is not set to NPWRTHRESH(02), this is a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting as specified following and proceed with the change.

NPPTHRESH(02)

CCI: CCI-000044

Group ID (Vulid): V-223879
Group Title: SRG-OS-000021-GPOS-00005
Rule ID: SV-223879r877720_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000060
Rule Title: The CA-TSS PTHRESH Control Option must be set to 2.
Legacy ID: V-98465
Legacy ID: SV-107569

Vulnerability Discussion: By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the PTHRESH Control Option value is not set to PTHRESH(02), this is a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting as specified following and proceed with the change.

PTHRESH(02)

CCI: CCI-000044

Group ID (Vulid): V-223880
Group Title: SRG-OS-000021-GPOS-00005
Rule ID: SV-223880r877721_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000070
Rule Title: The CA-TSS NPPTHRESH Control Option must be properly set.
Legacy ID: V-98467
Legacy ID: SV-107571

Vulnerability Discussion: By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the PTHRESH Control Option value is not set to NPPTHRESH(02), this is a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting as specified following and proceed with the change.

NPPTHRESH(02)

CCI: CCI-000044

Group ID (Vulid): V-223881
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-223881r877722_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000080
Rule Title: IBM z/OS must limit access for SMF collection files (i.e., SYS1.MANx) to appropriate users and/or batch jobs that perform SMF dump processing.
Legacy ID: V-98469
Legacy ID: SV-107573

Vulnerability Discussion: SMF data collection is the system activity journaling facility of the

z/OS system. Unauthorized access could result in the compromise of logging and recording of the operating system environment, ESM, and customer data.

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality. Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit operating system activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029, SRG-OS-000256-GPOS-00097, CCI-001494, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000080-GPOS-00048, SRG-OS-000206-GPOS-00084, SRG-OS-000324-GPOS-00125

Check Content:
Refer to the SMFPRMxx member in SYS1.PARMLIB. Determine the SMF and/or Logstream data set name.

If the following statements are true, this is not a finding.

-The ESM data set rules for the SMF data collection files (e.g., SYS1.MAN* or IFASMF.SYS1.*) restrict ALTER access to only z/OS systems programming personnel.
-The ESM data set rules for the SMF data collection files (e.g., SYS1.MAN* or IFASMF.SYS1.*) restrict UPDATE access to z/OS systems programming personnel, and/or batch jobs that perform SMF dump processing and others as approved by ISSM.
-The ESM data set rules for the SMF data collection files (e.g., SYS1.MAN* or IFASMF.SYS1.*) restrict READ access to auditors and others approved by the ISSM.
-The ESM data set rules for SMF data collection files (e.g., SYS1.MAN* or IFASMF.SYS1.*) specify that all (i.e., failures and successes) UPDATE and/or ALTER access are logged.

Fix Text: Ensure that allocate/alter authority to SMF collection files is limited to only systems programming staff and and/or batch jobs that perform SMF dump processing; access can be granted to others as determined by ISSM.

Ensure that read access is limited to auditors. Access may be granted to others as determined by the ISSM.

Ensure the accesses are being logged.

Ensure that all (i.e., failures and successes) WRITE or greater access are logged.

Ensure read access failures are logged.

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-000165

CCI: CCI-000213

CCI: CCI-001314

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

CCI: CCI-002235

Group ID (Vulid): V-223882
Group Title: SRG-OS-000063-GPOS-00032
Rule ID: SV-223882r877723_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000090
Rule Title: IBM z/OS SYS1.PARMLIB must be properly protected.
Legacy ID: V-98471
Legacy ID: SV-107575

Vulnerability Discussion: Without the capability to restrict which roles and individuals can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events. Misconfigured audits may degrade the system's performance by overwhelming the audit log. Misconfigured audits may also make it more difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Satisfies: SRG-OS-000063-GPOS-00032, SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100, SRG-OS-000362-GPOS-00149, SRG-OS-000337-GPOS-00129, SRG-OS-000324-GPOS-00125

Check Content:
Execute a data set list of access to SYS1.PARMLIB.

If the ESM data set rules for SYS1.PARMLIB allow inappropriate (e.g., global READ) access, this is a finding.

If data set rules for SYS1.PARMLIB do not restrict READ, WRITE or greater access to only systems programming personnel, this is a finding.

If data set rules for SYS1.PARMLIB do not restrict READ and UPDATE access to only domain level security administrators, this is a finding.

If data set rules for SYS1.PARMLIB do not restrict READ access to only system Level Started Tasks, authorized Data Center personnel, and auditors, this is a finding.

If data set rules for SYS1.PARMLIB do not specify that all (i.e., failures and successes) WRITE or greater access will be logged, this is a finding.

Fix Text: Ensure the accesses are being logged.

CCI: CCI-000171

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-001812

CCI: CCI-001914

CCI: CCI-002235

Group ID (Vulid): V-223883
Group Title: SRG-OS-000067-GPOS-00035
Rule ID: SV-223883r877725_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000100

Rule Title: IBM z/OS for PKI-based authentication must use ICSF or the ESM to store keys.
Legacy ID: V-98473
Legacy ID: SV-107577

Vulnerability Discussion: If the private key is discovered, an attacker can use the key to authenticate as an authorized user and gain access to the network infrastructure.

The cornerstone of the PKI is the private key used to encrypt or digitally sign information.

If the private key is stolen, this will lead to the compromise of the authentication and non-repudiation gained through PKI because the attacker can use the private key to digitally sign documents and pretend to be the authorized user.

Both the holders of a digital certificate and the issuing authority must protect the computers, storage devices, or whatever they use to keep the private keys.

Check Content:
Any keys or Certificates must be managed in ICSF or the external security manager and not in UNIX files.

From the ISPF Command Shell enter:
OMVS
enter
find / -name *.kdb
and
Find / -name *.jks

If any files are present, this is a finding.

OMVS
enter
find / -name *.kdb
and
Find / -name *.jks

If any files are present, this is a finding.

Fix Text: Define all Keys/Certificates to ICSF or the security database.

Remove all .kdb and .jks key files.

CCI: CCI-000186

Group ID (Vulid): V-223885
Group Title: SRG-OS-000069-GPOS-00037
Rule ID: SV-223885r877726_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000120
Rule Title: The CA-TSS NEWPHRASE and PPSCHAR Control Options must be properly set.
Legacy ID: SV-107581
Legacy ID: V-98477

Vulnerability Discussion: Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Satisfies: SRG-OS-000069-GPOS-00037, SRG-OS-000070-GPOS-00038

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the NEWPHRASE Control Option conforms to the following requirements, this is not a finding.

MA=1-32
MN=1-32
ID
MAX=100
MIN=15-100
MINDAYS=1
NR=0-1
SC=1-32
WARN=1-10

If the PPSCHAR Control Option conform to the allowable list defined in CA Top Secret for z/OS Control Options Guide, this is not a finding.

Note: These characters will be specified at a minimum. "40" represents the blank character. Characters can be identified by their character or hex equivalent.

Fix Text: Note: Support of mixed case passwords can only be set when the security file has been copied by TSSXTEND with the option NEWPWBLOCK.

Configure the NEWPHRASE Control Option values to the following requirements:

MA=1-32
MN=1-32
ID
MAX=100
MIN=15-100
MINDAYS=1
NR=0-1
SC=1-32
WARN=1-10

Configure the PPSCHAR Control Option to the allowable list defined in CA Top Secret for z/OS User Guide.

Note: These characters will be specified at a minimum. "40" represents the blank character. Characters can be identified by their character or hex equivalent.

Example:

TSS MODIFY
NEWPHRASE(MA=1,MN=1,ID,MAX=100,MIN=15,MINDAYS=1,NR=1,SC=1,WARN=10)
TSS MODIFY PPSCHAR(c,c,c,c,...)

(Use the allowable list defined in CA Top Secret for z/OS Control Options Guide.)

CCI: CCI-000192

CCI: CCI-000193

Group ID (Vulid): V-223886
Group Title: SRG-OS-000071-GPOS-00039
Rule ID: SV-223886r877727_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000130
Rule Title: The CA-TSS NEWPW control options must be properly set.
Legacy ID: V-98479
Legacy ID: SV-107583

Vulnerability Discussion: If the private key is stolen, this will lead to the compromise of the authentication and non-repudiation gained through PKI because the attacker can use the private key to digitally sign documents and pretend to be the authorized user.

Satisfies: SRG-OS-000071-GPOS-00039, SRG-OS-000072-GPOS-00040, SRG-OS-000075-GPOS-00043, SRG-OS-000480-GPOS-00225, SRG-OS-000266-GPOS-00101, SRG-OS-000279-GPOS-00109

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the NEWPW Control Option values conform to the following requirements, this is not a finding.

NEWPW(MIN=8,WARN=10, MINDAYS=1, NR=0, ID, TS, SC, RS, FA, FN, MC, UC, LC)

NOTE: For the Option SC, the PASSCHAR control option should be set to the allowable list defined in CA Top Secret for z/OS Control Options Guide.

NOTE: For the Option RS, at a minimum use the reserved word prefix list found in the site security plan.

Fix Text: Note: Support of mixed case passwords can only be set when the security file has been copied by TSSXTEND with the option NEWPWBLOCK.

Configure the NEWPW Control Option values conform to the following requirements:

NEWPW(MIN=8,WARN=10, MINDAYS=1, NR=0, ID, TS, SC, RS, FA, FN, MC, UC, LC)

NOTE: For the Option SC, the PASSCHAR control option should be set to the allowable list defined in CA Top Secret for z/OS Control Options Guide.

NOTE: For the Option RS, at a minimum use the reserved word prefix list found in the site security plan.

CCI: CCI-000194

CCI: CCI-000195

CCI: CCI-000198

CCI: CCI-000366

CCI: CCI-001619

CCI: CCI-002361

Group ID (Vulid): V-223887
Group Title: SRG-OS-000073-GPOS-00041
Rule ID: SV-223887r877728_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000140
Rule Title: IBM z/OS must use NIST FIPS-validated cryptography to protect passwords in the security database.
Legacy ID: V-98481
Legacy ID: SV-107585

Vulnerability Discussion: Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Satisfies: SRG-OS-000073-GPOS-00041, SRG-OS-000074-GPOS-00042

Check Content:
From the ISPF command shell line enter:
TSS MODIFY(STATUS)

If either of the following is included, this is not a finding.

AES_ENCRYPTION(Active,128)
AES_ENCRYPTION(Active,256)

Fix Text: Evaluate the impact associated with implementation of the control option.

Develop a plan of action to implement the control option as specified below:

Convert passwords/password phrases from Triple-DES encryption to 128-bit AES or 256-bit encryption by running TSSMAINT (with the AESENCRYPT option specified) and then running TSSXTEND to copy the old security file to the new security file.

Please consult CA-TSS Installation guide for more information.

CCI: CCI-000196

CCI: CCI-000197

Group ID (Vulid): V-223888
Group Title: SRG-OS-000076-GPOS-00044
Rule ID: SV-223888r877729_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000150
Rule Title: The CA-TSS PWEXP Control Option must be set to 60.
Legacy ID: SV-107587
Legacy ID: V-98483

Vulnerability Discussion: Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the PWEXP Control Option value is not set to PWEXP(60), this is a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the following control option setting as specified and proceed with the change.

PWEXP(60)

CCI: CCI-000199

Group ID (Vulid): V-223889
Group Title: SRG-OS-000076-GPOS-00044
Rule ID: SV-223889r877730_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000160
Rule Title: The CA-TSS PPEXP Control Option must be properly set.

Legacy ID: SV-107589
Legacy ID: V-98485

Vulnerability Discussion: Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the PPEXP Control Option will conform to the following requirements, this is not a finding.

PPEXP(60)

Fix Text: Configure the PPEXP Control Option value to conform to the following requirements.

PPEXP(60)

Example:

TSS MODIFY PPEXP(60)

CCI: CCI-000199

Group ID (Vulid): V-223890
Group Title: SRG-OS-000077-GPOS-00045
Rule ID: SV-223890r877731_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000170
Rule Title: The CA-TSS PWHIST Control Option must be set to 10 or greater.
Legacy ID: SV-107591
Legacy ID: V-98487

Vulnerability Discussion: Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. If the information system or application allows the user to consecutively reuse their password when that password has exceeded its defined lifetime, the end result is a password that is not changed as per policy requirements.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the PWHIST Control Option value is not set to PWHIST(10) or greater, this is a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the following control option setting as specified and proceed with the change.

PWHIST(10) or greater

CCI: CCI-000200

Group ID (Vulid): V-223891
Group Title: SRG-OS-000077-GPOS-00045
Rule ID: SV-223891r877732_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000180
Rule Title: The CA-TSS PPHIST Control Option must be properly set.
Legacy ID: SV-107593
Legacy ID: V-98489

Vulnerability Discussion: Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. If the information system or application allows the user to consecutively reuse their password when that password has exceeded its defined lifetime, the end result is a password that is not changed as per policy requirements.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the PPHIST Control Option conforms to the following requirements, this is not a finding.

PPHIST(10-64)

Fix Text: Configure the PPHIST Control Option value to conforms to the following requirements:

PPHIST(10-64)

Example:

TSS MODIFY PPHIST(10)

CCI: CCI-000200

Group ID (Vulid): V-223892
Group Title: SRG-OS-000078-GPOS-00046
Rule ID: SV-223892r877733_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000190
Rule Title: The IBM z/OS operating system must enforce a minimum eight-character password length.
Legacy ID: SV-107595
Legacy ID: V-98491

Vulnerability Discussion: The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the NEWPW Control Option values conform to the following requirements, this is not a finding.

NEWPW(MIN=8,WARN=10, MINDAYS=1, NR=0, ID, TS, SC, RS, FA, FN, MC, UC, LC)

NOTE: For the Option SC, the PASSCHAR control option should be set to the allowable list defined in CA Top Secret for z/OS Control Options Guide.

NOTE: For the Option RS, at a minimum use the reserved word prefix list found in the site security plan.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a

plan of action to implement the control option setting as specified and proceed with the change.

(Support of mixed case passwords can only be set when the security file has been copied by TSSXTEND with the option NEWPWBLOCK.)

Configure the NEWPW Control Option values to conform to the following requirements:

NEWPW(MIN=8,WARN=10, MINDAYS=1, NR=0, ID, TS, SC, RS, FA, FN, MC, UC, LC)

NOTE: For the Option SC, the PASSCHAR control option should be set to the allowable list defined in CA Top Secret for z/OS Control Options Guide.

NOTE: For the Option RS, at a minimum use the reserved word prefix list found in the site security plan.

CCI: CCI-000205

Group ID (Vulid): V-223893
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223893r877734_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000200
Rule Title: CA-TSS access to SYS1.LINKLIB must be properly protected.
Legacy ID: SV-107597
Legacy ID: V-98493

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100, SRG-OS-000362-

GPOS-00149, SRG-OS-000324-GPOS-00125

Check Content:
Execute a data set list of access to SYS1.LINKLIB.

If the ESM data set rules for SYS1.LINKLIB allow inappropriate (e.g., global READ) access, this is a finding.

If data set rules for SYS1.LINKLIB do not restrict READ, WRITE or greater access to only systems programming personnel, this is a finding.

If data set rules for SYS1.LINKLIB do not restrict READ and UPDATE access to only domain level security administrators, this is a finding.

If data set rules for SYS1.LINKLIB do not restrict READ access to only system Level Started Tasks, authorized Data Center personnel, and auditors, this is a finding.

If data set rules for SYS1.LINKLIB do not specify that all (i.e., failures and successes) WRITE or greater access will be logged, this is a finding.

Fix Text: Configure the ESM rules for SYS1.LINKLIB limit access to system programmers only and all WRITE or greater access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-001812

Group ID (Vulid): V-223894
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223894r877735_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000210
Rule Title: CA-TSS must limit Write or greater access to SYS1.SVCLIB to system programmers only.
Legacy ID: SV-107599
Legacy ID: V-98495

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information

by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100, SRG-OS-000324-GPOS-00125

Check Content:
Execute a data set list of access for SYS1.SVCLIB.

If all of the following are true, this is not a finding.

If any of the following are untrue, this is a finding.

ESM data set rules for SYS1.SVCLIB restrict WRITE or greater access to only z/OS systems programming personnel.
ESM data set rules for SYS1.SVCLIB specify that all (i.e., failures and successes) WRITE or greater access will be logged.

Fix Text: Configure WRITE or greater access to SYS1.SVCLIB to be limited to system programmers only and all WRITE or greater access is logged and reviewed. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes for SYS1.SVCLIB. SYS1.SVCLIB contains SVCs and I/O appendages as such: they are very powerful and will be strictly controlled to avoid compromising system integrity.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223895
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223895r877736_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000220
Rule Title: CA-TSS must limit Write or greater access to SYS1.IMAGELIB to system programmers only.
Legacy ID: SV-107601
Legacy ID: V-98497

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100, SRG-OS-000324-GPOS-00125

Check Content:
Execute a data set list of access for SYS1.IMAGELIB.

If the following guidance is true, this is not a finding.

The ACP data set rules for SYS1.IMAGELIB do not restrict WRITE or greater access to only systems programming personnel.
The ACP data set rules for SYS1.IMAGELIB do not specify that all (i.e., failures and successes) WRITE or greater access will be logged.

Fix Text: Configure WRITE or greater access to SYS1.IMAGELIB to be limited to system programmers only and all WRITE or greater access is logged.

Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required to protect SYS1.IMAGELIB.

SYS1.IMAGELIB is automatically APF-authorized. This data set contains modules, images, tables, and character sets which are essential to system print services.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223896
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223896r877737_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000230
Rule Title: CA-TSS must limit Write or greater access to SYS1.LPALIB to system programmers only.
Legacy ID: SV-107603
Legacy ID: V-98499

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100, SRG-OS-000324-GPOS-00125

Check Content:
Execute a data set list of access for SYS1.LPALIB.

If all of the following are untrue, this is a finding.

If any of the following is true, this is a finding.

The ESM data set rules for SYS1.LPALIB do not restrict WRITE or greater access to only z/OS systems programming personnel.
The ESM data set rules for SYS1.LPALIB do not specify that all (i.e., failures and successes) WRITE or greater access will be logged.

Fix Text: Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to protect SYS1.LPALIB.

Configure WRITE or greater access to SYS1.LPALIB to be limited to system programmers only and all WRITE or greater access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223897
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223897r877738_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000240
Rule Title: CA-TSS must limit WRITE or greater access to all APF-authorized libraries to system programmers only.
Legacy ID: V-98501
Legacy ID: SV-107605

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not

automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100, SRG-OS-000324-GPOS-00125

Check Content:
From Any ISPF input line, enter TSO ISRDDN APF.

If all of the following are untrue, this is not a finding.

If any of the following are true, this is a finding.

The ACP data set rules for APF libraries do not restrict WRITE or greater access to only z/OS systems programming personnel.
The ACP data set rules for APF libraries do not specify that all (i.e., failures and successes) WRITE or greater access will be logged.

Fix Text: Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to protect APF Authorized Libraries.

Configure WRITE or greater access to all APF-authorized libraries to be limited to system programmers only and all WRITE or greater access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223898

Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223898r877739_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000250
Rule Title: IBM z/OS libraries included in the system REXXLIB concatenation must be properly protected.
Legacy ID: V-98503
Legacy ID: SV-107607

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100, SRG-OS-000324-GPOS-00125

Check Content:
Refer to AXRxx member of PARMLIB for each REXXLIB ADD statement.

If the ESM data set rules for libraries in the REXXLIB concatenation restrict WRITE or greater access to only z/OS systems programming personnel, this is not a finding.

If the ESM data set rules for libraries in the REXXLIB concatenation restrict READ access to the following, this is not a finding.

Appropriate Started Tasks
Auditors
The user-id defined in PARMLIB member AXR00 AXRUSER(user-id)

If the ESM data set rules for libraries in the REXXLIB concatenation specify that all (i.e., failures and successes) WRITE or greater access will be logged, this is not a finding.

Fix Text: Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to protect APF Authorized Libraries.

Configure ESM data set rules to limit WRITE or greater access to libraries included in the system REXXLIB concatenation to system programmers only.
Configure ESM data set rules allow READ access to only appropriate Started Tasks and Auditors.
Configure ESM data set rules to log WRITE or greater access (i.e., successes and failures).

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223899
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223899r877740_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000260
Rule Title: CA-TSS must limit Write or greater access to all LPA libraries to system programmers only.
Legacy ID: V-98505
Legacy ID: SV-107609

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100, SRG-OS-000324-GPOS-00125

Check Content:
From any ISPF input line, enter TSO ISRDDN LPA.

If all of the following are untrue, this is not a finding.

If any of the following is true, this is a finding.

The ACP data set rules for LPA libraries do not restrict WRITE or greater access to only z/OS systems programming personnel.
The ACP data set rules for LPA libraries do not specify that all (i.e., failures and successes) WRITE or greater access will be logged.

Fix Text: Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to protect LPA Libraries.

Configure the WRITE or greater access to all LPA libraries to be limited to system programmers only and all WRITE or greater access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223900
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223900r877741_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000270
Rule Title: CA-TSS must limit Write or greater access to SYS1.NUCLEUS to system programmers only.
Legacy ID: V-98507
Legacy ID: SV-107611

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web

servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100, SRG-OS-000324-GPOS-00125

Check Content:
Execute a dataset list of access for SYS1.NUCLEUS.

If all of the following are untrue, there is not a finding.

If any of the following is true, this is a finding.

The ACP data set rules for SYS1.NUCLEUS do not restrict WRITE or greater access to only z/OS systems programming personnel.
The ACP data set rules for SYS1.NUCLEUS do not specify that all (i.e., failures and successes) WRITE or greater access will be logged.

Fix Text: Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to protect SYS1.NUCLEUS.

Configure the WRITE or greater access to SYS1.NUCLEUS to be limited to system programmers only and all WRITE or greater access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223901
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223901r877742_rule
Severity: CAT III
Rule Version (STIG-ID): TSS0-ES-000280
Rule Title: CA-TSS must limit Write or greater access to libraries that contain PPT modules to system programmers only.
Legacy ID: V-98509
Legacy ID: SV-107613

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100, SRG-OS-000324-GPOS-00125

Check Content:
Review program entries in the IBM Program Properties Table (PPT). You may use a third-party product to examine these entries however, to determine program entries issue the following command from an ISPF command line:
TSO ISRDDN LOAD IEFSDPPT
Press Enter.

For each module identified in the "eyecatcher" if all of the following are untrue, this is not a finding.

If any of the following is true, this is a finding.

The ACP data set rules for libraries that contain PPT modules do not restrict WRITE or greater

access to only z/OS systems programming personnel.
The ACP data set rules for libraries that contain PPT modules do not specify that all WRITE or greater access will be logged.

Fix Text: Configure the WRITE or greater access to libraries containing PPT modules to be limited to system programmers only and all WRITE or greater access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223902
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223902r877743_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000290
Rule Title: CA-TSS must limit WRITE or greater access to LINKLIST libraries to system programmers only.
Legacy ID: V-98511
Legacy ID: SV-107615

Vulnerability Discussion: Preventing non-privileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100, SRG-OS-000324-GPOS-00125

Check Content:
From any ISPF input line, enter TSO ISRDDN LINKLIST.

If all of the following are untrue, this is not a finding.

If any of the following is true, this is a finding.

The ACP data set rules for LINKLIST libraries do not restrict WRITE or greater access to only z/OS systems programming personnel.

The ACP data set rules for LINKLIST libraries do not specify that all (i.e., failures and successes) WRITE or greater access will be logged.

Fix Text: Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required to protect the LINKLIST libraries.

Configure the WRITE or greater access to LINKLIST libraries to be limited to system programmers only and all WRITE or greater access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223903
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223903r877744_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000300
Rule Title: CA-TSS security data sets and/or databases must be properly protected.
Legacy ID: V-98513
Legacy ID: SV-107617

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000134-GPOS-00068, SRG-OS-000259-GPOS-00100, SRG-OS-000324-GPOS-00125

Check Content:
Determine all associated ESM security data sets and/or databases.

If the following accesses to the ESM security data sets and/or databases are properly restricted as detailed below, this is not a finding.

The ESM data set rules for ESM security data sets and/or databases restrict READ access to auditors and DASD batch.

The ESM data set rules for ESM security data sets and/or databases restrict READ and/or greater access to z/OS systems programming personnel, security personnel, and/or batch jobs that perform ESM maintenance.

All (i.e., failures and successes) data set access authorities (i.e., READ, UPDATE, ALTER, and CONTROL) for ESM security data sets and/or databases are logged.

Fix Text: Review access authorization to critical security database files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to protect the ESM files.

Configure READ and/or greater access to all ESM files and/or databases are limited to system programmers and/or security personnel, and/or batch jobs that perform ESM maintenance. READ access can be given to auditors and DASD batch. All accesses to ESM files and/or databases are logged.

CCI: CCI-000213

CCI: CCI-001084

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223904
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223904r877745_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000310
Rule Title: CA-TSS must limit access to the System Master Catalog to appropriate authorized users.
Legacy ID: V-98515
Legacy ID: SV-107619

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000324-GPOS-00125

Check Content:
Refer to SYSCATxx member of SYS1.NUCLEUS.

Multiple SYSCATxx members may be defined; if so, refer to Master Catalog message for IPL.

If the member is not found, refer to the appropriate LOADxx member of SYS1.PARMLIB.

If data set rules for the Master Catalog do not restrict greater than "READ" access to only z/OS systems programming personnel, this is a finding.

If products or procedures requiring system programmer access for system-level maintenance meet the following specific case, this is not a finding:
- The batch job or procedure must be documented in the SITE Security Plan.
- Reside in a data set that is restricted to systems programmers' access only.

If data set rules for the Master Catalog do not specify that all (i.e., failures and successes) greater than "READ" access will be logged, this is a finding.

Fix Text: Review access authorization to critical system files.

Evaluate the impact of correcting the deficiency.

Develop a plan of action and implement the changes as required to protect the MASTER CATALOG.

Configure the ESM rules for system catalog to only allow access above "READ" to systems programmers and those authorized by the ISSM/ISSO.

Configure ESM rules for the master catalog to allow access above "READ" to systems programmers ONLY.

Configure ESM rules for the master catalog to allow any products or procedures system programmer access for system-level maintenance that meet the following specific case:
- The batch job or procedure must be documented in the SITE Security Plan.
- Reside in a data set that is restricted to systems programmers' access only.

All greater than read access must be logged.

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223905
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223905r877746_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000320
Rule Title: CA-TSS allocate access to system user catalogs must be limited to system programmers only.
Legacy ID: V-98517
Legacy ID: SV-107621

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not

automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000324-GPOS-00125

Check Content:
From the ISPF Command Shell enter:
LISTCat USERCATALOG ALL NOPREFIX

Review the ESM data set rules for each usercatalog defined.

If the data set rules for User Catalogs do not restrict ALTER access to only z/OS systems programming personnel, this is a finding.

If products or procedures requiring system programmer access for system-level maintenance meet the following specific case, this is not a finding:
- The batch job or procedure must be documented in the SITE Security Plan.
- Reside in a data set that is restricted to systems programmers' access only.

If the data set rules for User Catalogs do not specify that all (i.e., failures and successes) ALTER access will be logged, this a finding.

Note: If the USER CATALOGS contain SMS managed data sets, READ access is sufficient to allow user operations. If the USER CATALOGS do not contain SMS managed data sets, UPDATE access is required for user operation.

Fix Text: Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required to protect USER CATALOGS.

Configure ESM rules for allocate access to USER CATALOGS, limited to system programmers only, and all allocate access is logged.

Configure ESM rules for the USER CATALOGS to allow any products or procedures system programmer access for system-level maintenance that meet the following specific case:
- The batch job or procedure must be documented in the SITE Security Plan.

- Reside in a data set that is restricted to systems programmers' access only.

Note: If the USER CATALOGS contain SMS managed data sets, READ access is sufficient to allow user operations. If the USER CATALOGS do not contain SMS managed data sets, UPDATE access is required for user operation.

CCI: CCI-000213

Group ID (Vulid): V-223906
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223906r877747_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000330
Rule Title: CA-TSS must limit WRITE or greater access to all system-level product installation libraries to system programmers only.
Legacy ID: SV-107623
Legacy ID: V-98519

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100, SRG-OS-000324-GPOS-00125

Check Content:
Have the systems programmer for z/OS supply the following information:

The data set name and associated SREL for each SMP/E CSI utilized to maintain this system.

The data set name of all SMP/E TLIBs and DLIBs used for installation and production support. A comprehensive list of the SMP/E DDDEFs for all CSIs may be used if valid.

The ACP data set rules for system-level product installation libraries (e.g., SMP/E CSIs) allow inappropriate access.

The ACP data set rules for system-level product installation libraries (e.g., SMP/E CSIs) do not restrict WRITE or greater access to only z/OS systems programming personnel.

If all of the above are untrue, this is not a finding.

If any of the above is true, or if these data sets cannot be identified due to a lack of requested information, this is a finding.

Fix Text: Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required to protect System-level product installation libraries.

Configure allocate access to all system-level product execution libraries to be limited to system programmers only.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223907
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223907r877748_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000340
Rule Title: CA-TSS must limit WRITE or greater access to the JES2 System data sets (e.g., Spool, Checkpoint, and Initialization parameters) to system programmers only.
Legacy ID: V-98521
Legacy ID: SV-107625

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not

automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100, SRG-OS-000324-GPOS-00125

Check Content:
The ESM data set rules for the JES2 System data sets (e.g., Spool, Checkpoint, and Initialization parameters) do not restrict WRITE or greater access to only z/OS systems programming personnel.

The ESM data set rules for the JES2 System data sets (e.g., Spool, Checkpoint, and Initialization parameters) allow inappropriate access not documented and approved by ISSO.

If both of the above are untrue, this is not a finding.

If either of the above is true, this is a finding.

Fix Text: Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required to protect JES2 System data sets (spool, checkpoint, and parmlib data sets).

Configure WRITE or greater access to JES2 System data sets (spool, checkpoint, and parmlib data sets) to be limited to system programmers only.
Access other than this should be documented and approved by the ISSO. (Example: All SYS1.HASP* data sets.)

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223908
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223908r877749_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000350
Rule Title: CA-TSS must limit Write or greater access to SYS1.UADS to system programmers only, and Read and Update access must be limited to system programmer personnel and/or security personnel.
Legacy ID: V-98523
Legacy ID: SV-107627

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000324-GPOS-00125

Check Content:
The ESM data set rules for SYS1.UADS restricts WRITE or Greater access to only z/OS systems programming personnel.

The ESM data set rules for SYS1.UADS restricts READ and/or UPDATE access to z/OS systems programming personnel and/or security personnel.

The ESM data set rules for SYS1.UADS specifies that all (i.e., failures and successes) data set access authorities (i.e., READ, UPDATE, ALTER, and CONTROL) will be logged.

The ESM data set rules for SYS1.UADS restricts READ access to auditors as documented in Security Plan.

If all of the above are untrue, this is not a finding.

If any of the above is true, this is a finding.

Fix Text: Evaluate the impact of correcting any deficiency. Develop a plan of action and implement the changes as required to protect SYS1.UADS.

SYS1.UADS WRITE or Greater authority is limited to the systems programming staff.

Read and update access should be limited to the security staff.

READ access is limited to Auditors when included in the site security plan

Configure allocate access to SYS1.UADS to be limited to system programmers only, read and update access to SYS1.UADS to be limited to system programmer personnel and/or security personnel and all data set access is logged.

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223909
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223909r877750_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000360
Rule Title: CA-TSS must limit access to data sets used to back up and/or dump SMF collection files to appropriate users and/or batch jobs that perform SMF dump processing.
Legacy ID: SV-107629
Legacy ID: V-98525

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000206-GPOS-00084, SRG-OS-000324-GPOS-00125

Check Content:
Obtain the procedures and collection specifics for SMF data sets and backup.

If the ESM data set rules for the SMF dump/backup files do not restrict WRITE or greater access

to authorized DISA and site personnel (e.g., systems programmers and batch jobs that perform SMF processing), this is a finding.

If the ESM data set rules for the SMF dump/backup files do restrict update access as documented in the site security plan, this is a finding.

If the ESM data set rules for the SMF dump/backup files do not restrict READ access to auditors and others approved by the ISSM, this is a finding.

If the ESM data set rules for SMF dump/backup files do not specify that all (i.e., failures and successes) WRITE or greater access will be logged, this is a finding.

Fix Text: Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required to protect data sets used to backup and/or dump SMF Collection Files.

Configure data set rules for the SMF dump/backup files to restrict WRITE or greater access to authorized DISA and site personnel (e.g., systems programmers and batch jobs that perform SMF processing).

Configure data set rules for the SMF dump/backup files to restrict UPDATE access to others approved the ISSM.

Configure data set rules for the SMF dump/backup files to restrict READ access to authorized auditors and others approved by the ISSM.

Ensure that all update and alter access authority to SMF history files will be logged using the ESM's facilities.

CCI: CCI-000213

CCI: CCI-001314

CCI: CCI-002235

Group ID (Vulid): V-223910
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223910r877751_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000370
Rule Title: CA-TSS must limit access to SYSTEM DUMP data sets to system programmers only.

Legacy ID: SV-107631
Legacy ID: V-98527

Vulnerability Discussion: System DUMP data sets are used to record system data areas and virtual storage associated with system task failures. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100, SRG-OS-000324-GPOS-00125

Check Content:
Refer to data sets SYS1.DUMPxx, additionally, Dump data sets can be identified by reviewing the logical parmlib concatenation data sets for the current COMMNDxx member. Find the COM= which specifies the DUMPDS NAME (DD NAME=name-pattern) entry. The name-pattern is used to identify additional Dump data sets.

If the ESM data set rules for System Dump data sets do not restrict READ, UPDATE, and/or ALTER access to only systems programming personnel, this is a finding.

If the ESM data set rules for all System Dump data sets do not restrict READ access to personnel having justification to review these dump data sets, this is a finding.

Fix Text: Configure data set rules for access to SYSTEM DUMP data set(s) to be limited to system programmers only, unless a letter justifying access is filed with the ISSO in the site security plan.

Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to restrict access to these data sets.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223911
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223911r877752_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000380

Rule Title: CA-TSS WRITE or Greater access to System backup files must be limited to system programmers and/or batch jobs that perform DASD backups.
Legacy ID: SV-107633
Legacy ID: V-98529

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000324-GPOS-00125

Check Content:
Collect from the storage management group the identification of the DASD backup files and all associated storage management ACIDs.

If ESM data set rules for system DASD backup files do not restrict WRITE or greater access to z/OS systems programming and/or batch jobs that perform DASD backups this is a finding.

If READ Access to system backup data sets is not limited to auditors and others approved by the ISSM this is a finding.

Fix Text: Obtain the high level indexes to backup data sets names define their access to be restricted by the System's ESM to System Programmers and batch jobs that perform the backups. Define READ Access to system backup data sets to be limited to auditors and others approved by the ISSM.

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223912
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223912r877753_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000390
Rule Title: CA-TSS must limit access to SYS(x).TRACE to system programmers only.
Legacy ID: SV-107635
Legacy ID: V-98531

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000324-GPOS-00125

Check Content:
Execute a dataset list of access for SYS(x).TRACE files.

If the ESM data set rule for SYS1.TRACE restricts access to systems programming personnel and started tasks that perform GTF processing, this is not a finding.

If the ESM data set rule for SYS1.TRACE restricts access to others as documented and approved by ISSM, this is not a finding.

Fix Text: Configure the ESM access to SYS1.TRACE to be limited to system programmers or started tasks that perform GTF processing.
Other user access can be granted as documented and approved by the ISSM.

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223913
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223913r877754_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000400
Rule Title: CA-TSS must limit access to System page data sets (i.e., PLPA, COMMON, and LOCALx) to system programmers only.
Legacy ID: SV-107637
Legacy ID: V-98533

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000324-GPOS-00125

Check Content:
Execute a dataset list of access for System page data sets (i.e., PLPA, COMMON, and LOCALx).

If ESM data set rules for system page data sets (PLPA, COMMON, and LOCAL) restrict access to only systems programming personnel, this is not a finding.

If ESM data set rules for system page data sets (PLPA, COMMON, and LOCAL) restrict auditors to READ only, this is not a finding.

Fix Text: Configure the ESM data set rules for system page data sets (PLPA, COMMON, and

LOCAL) to restrict access to only systems programming personnel.

Auditors may be allowed READ Access as approved by the ISSM.

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223914
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223914r877755_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000410
Rule Title: CA-TSS must limit WRITE or greater access to libraries containing EXIT modules to system programmers only.
Legacy ID: SV-107639
Legacy ID: V-98535

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100, SRG-OS-000324-GPOS-00125

Check Content:
Examine the system for active exit modules. You may need the system administrator's help for this. There are third-party software products that can determine standard and dynamic exits loaded in the system.

If all the exits are found within APF, LPA, and LINKLIST, this is not applicable.

If ESM data set rules for libraries that contain system exit modules restrict WRITE or greater access to only z/OS systems programming personnel, this is not a finding.

If the ESM data set rules for libraries that contain exit modules specify that all WRITE or greater access will be logged, this is not a finding.

Fix Text: Using the ESM, protect the data sets associated with all product exits installed in the z/OS environment. This reduces the potential of a hacker adding a routine to a library and possibly creating an exposure. Confirm that all exits are tracked using a CMP. Develop usermods to include the source/object code used to support the exits. Have systems programming personnel review all z/OS and other product exits to confirm that the exits are required and are correctly installed.

Configure ESM data set rules for all WRITE or greater access to libraries containing z/OS and other system-level exits will be logged using the ACP's facilities. Only systems programming personnel will be authorized to update the libraries containing z/OS and other system level exits.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223915
Group Title: SRG-OS-000324-GPOS-00125
Rule ID: SV-223915r877756_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000420
Rule Title: CA-TSS must limit all system PROCLIB data sets to system programmers only and appropriate authorized users.
Legacy ID: SV-107641
Legacy ID: V-98537

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000324-GPOS-00125, SRG-OS-000080-GPOS-00048

Check Content:
Refer to the following for the PROCLIB data sets that contain the STCs and TSO logons from the following sources:

-MSTJCLxx member used during an IPL. The PROCLIB data sets are obtained from the IEFPDSI and IEFJOBS DD statements.

-PROCxx DD statements and JES2 Dynamic PROCLIBs. Where 'xx' is the PROCLIB entries for the STC and TSU JOBCLASS configuration definitions.

Verify that the accesses to the above PROCLIB data sets are properly restricted. If the following guidance is true, this is not a finding.

If the ESM data set access authorizations restrict READ access to all authorized users, this is not a finding.

If the ESM data set access authorizations restrict WRITE and/or greater access to systems programming personnel, this is not a finding.

Fix Text: Configure ESM data set rules to restrict all WRITE and/or greater access to all PROCLIBs referenced in the Master JCL and JES2 or JES3 procedure for started tasks (STCs) and TSO logons to systems programming personnel only.

Suggestion on how to update system to be compliant with this vulnerability:

NOTE: All examples are only examples and may not reflect your operating environment.

Obtain only the PROCLIB data sets that contain STC and TSO procedures. The data sets to be reviewed are obtained using the following steps:

-All data sets contained in the MSTJCLxx member in the DD statement concatenation for IEFPDSI and IEFJOBS.
-The data set in the PROCxx DD statement concatenation that are within the JES2 procedure or identified in the JES2 dynamic PROCLIB definitions. The specific PROCxx DD statement that is used is obtained from the PROCLIB entry for the JOBCLASSes of STC and TSU. The following are the data sets the process will obtain for analysis:

MSTJCL00

```
//MSTJCL00 JOB MSGLEVEL=(1,1),TIME=1440
//EXEC PGM=IEEMB860,DPRTY=(15,15)
//STCINRDR DD SYSOUT=(A,INTRDR)
//TSOINRDR DD SYSOUT=(A,INTRDR)
//IEFPDSI DD DSN=SYS3.PROCLIB,DISP=SHR <<===
//DD DSN=SYS2.PROCLIB,DISP=SHR <<===
//DD DSN=SYS1.PROCLIB,DISP=SHR <<===
//SYSUADS DD DSN=SYS1.UADS,DISP=SHR
//SYSLBC DD DSN=SYS1.BRODCAST,DISP=SHR
```

JES2

```
//JES2 PROC
//IEFPROC EXEC PGM=HASJES20,PARM=NOREQ,
//DPRTY=(15,15),TIME=1440,PERFORM=9
//ALTPARM DD DISP=SHR,
//DSN=SYS1.PARMLIB(JES2BKUP)
//HASPPARM DD DISP=SHR,
//DSN=SYS1.PARMLIB(JES2PARM)
//PROC00 DD DSN=SYS3.PROCLIB,DISP=SHR <<===
//DD DSN=SYS2.PROCLIB,DISP=SHR <<===
//DD DSN=SYS1.PROCLIB,DISP=SHR <<===
//PROC01 DD DSN=SYS4.USERPROC,DISP=SHR
//DD DSN=SYS3.PROCLIB,DISP=SHR
//DD DSN=SYS2.PROCLIB,DISP=SHR
//DD DSN=SYS1.PROCLIB,DISP=SHR
//IEFRDER DD SYSOUT=*
//HASPLIST DD DDNAME=IEFRDER
```

JES2 initialization parameter JOBCLASS PROCLIB entries

```
JOBCLASS(*) ACCT=NO, /* ACCT # NOT REQUIRED (DEF.)*/
...
PROCLIB=01, /* DEFAULT TO //PROC01 DD (DEF.)*/
...
JOBCLASS(STC) AUTH=ALL, /* ALLOW ALL COMMANDS (DEF.)*/
...
PROCLIB=00, /* USE //PROC00 DD (DEF.)*/
...
JOBCLASS(TSU) AUTH=ALL, /* ALLOW ALL COMMANDS (DEF.)*/
...
PROCLIB=00, /* USE //PROC00 DD (DEF.)*/
...
```

PROCLIB data set that will be used in the access authorization process:

SYS3.PROCLIB
SYS2.PROCLIB
SYS1.PROCLIB

The following PROCLIB data set will NOT be used or evaluated:

SYS4.USERPROC

Recommendation for sites:

The following are recommendations for the sites to ensure only PROCLIB data sets that contain the STC and TSO procedures are protected.

-Remove all application PROCLIB data sets from MSTJCLxx and JES2 procedures. The customer will have all JCL changed to use the JCLLIB JCL statement to refer to the application PROCLIB data sets.

Example:

//USERPROC JCLLIB ORDER=(SYS4.USERPROC)

-Remove all access to the application PROCLIB data sets and only authorize system programming personnel WRITE and/or greater access to these data sets.

-Document the application PROCLIB data set access for the customers that require WRITE and/or greater access. Use this documentation as justification for the inappropriate access created by the scripts.

-Change MSTJCLxx and JES2 procedure to identify STC and TSO PROCLIB data sets separate from application PROCLIB data sets. The following is a list of actions that can be performed to accomplish this recommendation:

a. Ensure that MSTJCLxx contains only PROCLIB data sets that contain STC and TSO procedures.
b. If an application PROCLIB data set is required for JES2, ensure that the JES2 procedure specifies more than one PROCxx DD statement concatenation or identified in the JES2 dynamic PROCLIB definitions. Identify one PROCxx DD statement data set concatenation that contains the STC and TSO PROCLIB data sets. Identify one or more additional PROCxx DD statements that can contain any other PROCLIB data sets. The concatenation of the additional PROCxx DD statements can contain the same data sets that are identified in the PROCxx DD statement for STC and TSO. The following is an example of the JES2 procedure:

//JES2 PROC
//IEFPROC EXEC PGM=HASJES20,PARM=NOREQ,
//DPRTY=(15,15),TIME=1440,PERFORM=9

```
//ALTPARM DD DISP=SHR,
//DSN=SYS1.PARMLIB(JES2BKUP)
//HASPPARM DD DISP=SHR,
//DSN=SYS1.PARMLIB(JES2PARM)
//PROC00 DD DSN=SYS3.PROCLIB,DISP=SHR
//DD DSN=SYS2.PROCLIB,DISP=SHR
//DD DSN=SYS1.PROCLIB,DISP=SHR
//PROC01 DD DSN=SYS4.USERPROC,DISP=SHR
//DD DSN=SYS3.PROCLIB,DISP=SHR
//DD DSN=SYS2.PROCLIB,DISP=SHR
//DD DSN=SYS1.PROCLIB,DISP=SHR
//IEFRDER DD SYSOUT=*
//HASPLIST DD DDNAME=IEFRDER
```

c. Ensure that the JES2 configuration file is changed to specify that the PROCLIB entry for the STC and TSU JOBCLASSes point to the proper PROCxx entry within the JES2 procedure or JES2 dynamic PROCLIB definitions that contain the STC and/or TSO procedures. All other JOBCLASSes can specify a PROCLIB entry that uses the same PROCxx or any other PROCxx DD statement identified in the JES2 procedure or identified in the JES2 dynamic PROCLIB definitions. The following is an example of the JES2 initialization parameters:

```
JOBCLASS(*) ACCT=NO, /* ACCT # NOT REQUIRED (DEF.)*/
...
PROCLIB=01, /* DEFAULT TO //PROC01 DD (DEF.)*/
...
JOBCLASS(STC) AUTH=ALL, /* ALLOW ALL COMMANDS (DEF.)*/
...
PROCLIB=00, /* USE //PROC00 DD (DEF.)*/
...
JOBCLASS(TSU) AUTH=ALL, /* ALLOW ALL COMMANDS (DEF.)*/
...
PROCLIB=00, /* USE //PROC00 DD (DEF.)*/
...
```

d. Ensure that only system programming personnel are authorized WRITE and/or greater access to PROCLIB data sets that contain STC and TSO procedures.

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223916
Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223916r877757_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000430
Rule Title: CA-TSS must protect memory and privileged program dumps in accordance with proper security requirements.
Legacy ID: SV-107643
Legacy ID: V-98539

Vulnerability Discussion: Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
If the IEAABD. resource and/or generic equivalent is defined with no access and all access logged, this is not a finding.

If the IEAABD.DMPAUTH. resource and/or generic equivalent is defined with READ access limited to authorized users, this is not a finding.

If the IEAABD.DMPAUTH. resource and/or generic equivalent UPDATE or greater access is restricted to only systems personnel and all access is logged, this is not a finding.

If the IEAABD.DMPAKEY resource and/or generic equivalent is defined and all access is restricted to systems personnel and that all access is logged, this is not a finding.

Fix Text: Memory and privileged program dump resources are provided via resources in the FACILITY resource class. Ensure that the following are properly specified in the ESM.

(Note: The resources and/or resource prefixes identified below are examples of a possible installation. The actual resources and/or resource prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.)

Below is listed the access requirements for memory and privileged program dump resources. Ensure the guidelines for the resource type, resources, and/or generic equivalent are followed. When protecting the facilities for dumps lists via the FACILITY resource class, ensure that the following items are in effect:

IEAABD.
IEAABD.DMPAUTH.
IEAABD.DMPAKEY.

The RACF resource rules for the resources specify UACC(NONE) and NOWARNING.

Ensure that no access is given to IEAABD. resource.

Example

RDEF FACILITY IEAABD.** UACC(NONE) OWNER(owner group) AUDIT(ALL(READ))

IEAABD.DMPAUTH. READ access is limited to authorized users that have a valid job duties requirement for access. UPDATE access will be restricted to system programming personnel and access will be logged.

Example:

RDEF FACILITY IEAABD.DMPAUTH.** UACC(NONE) OWNER(owner group) AUDIT(ALL(UPDATE))

PERMIT IEAABD.DMPAUTH.** CLASS(FACILITY) ID(authusers) ACCESS(READ)
PERMIT IEAABD.DMPAUTH.** CLASS(FACILITY) ID(syspsmpl) ACCESS(UPDATE)

IEAABD.DMPAKEY. access will be restricted to system programming personnel and access will be logged.

Example:

RDEF FACILITY IEAABD.DMPAKEY.** UACC(NONE) OWNER(owner group) AUDIT(ALL(READ))

PERMIT IEAABD.DMPAKEY.** CLASS(FACILITY) ID(syspsmpl) ACCESS(READ)

CCI: CCI-000213

Group ID (Vulid): V-223917
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223917r877758_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000440
Rule Title: IBM z/OS must protect dynamic lists in accordance with proper security requirements.
Legacy ID: V-98541
Legacy ID: SV-107645

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information

by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000324-GPOS-00125

Check Content:
Refer to the CSV-prefixed resources defined below:

CSVAPF.
CSVAPF.MVS.SETPROG.FORMAT.DYNAMIC
CSVAPF.MVS.SETPROG.FORMAT.STATIC
CSVDYLPA.
CSVDYNEX.
CSVDYNEX.LIST
CSVDYNL.
CSVDYNL.UPDATE.LNKLST
CSVLLA.

If the TSS IBMFAC resource class in the RDT has the DEFPROT attribute specified and/or the CSV resources and/or generic equivalent are owned this is not a finding.

If the TSS resources and/or generic equivalent identified above are defined with ACTION(AUDIT) and UPDATE access restricted to system programming personnel this is not a finding.

If the TSS CSVDYNEX.LIST resource and/or generic equivalent is defined with ACTION(AUDIT) and UPDATE access restricted to system programming personnel this is a finding.

If the TSS CSVDYNEX.LIST resource and/or generic equivalent are defined with READ access restricted to auditors this is not a finding.

If the products CICS and/or CONTROL-O are on the system, and the TSS access to the CSVLLA resource access to the CSVLLA resource and/or generic equivalent are defined with ACTION(AUDIT) and UPDATE access restricted to the CICS and CONTROL-O STC ACIDs this is not a finding.

If any software product requires access to dynamic LPA updates on the system, the TSS access to the CSVDYLPA resource and/or generic equivalent will be defined with ACTION(AUDIT)

and UPDATE only after the product has been validated with the appropriate STIG or SRG for compliance AND receives documented and filed authorization that details the need and any accepted risks from the site ISSM or equivalent security authority.

Note: In the above, UPDATE access can be substituted with ALL or CONTROL. Review the permissions in the TSS documentation when specifying UPDATE.

Fix Text: Configure TSS to ensure that the Dynamic List resources are defined to the IBMFAC resource class and protected. Only system programmers and a limited number of authorized users and Approved authorized Started Tasks are able to issue these commands. All access is logged.

The required CSV-prefixed Facility Class resources are listed below. These resources or generic equivalents should be defined and permitted as required with only z/OS systems programmers and logging enabled. Minimum required list of CSV-prefixed resources:

CSVAPF.
CSVAPF.MVS.SETPROG.FORMAT.DYNAMIC
CSVAPF.MVS.SETPROG.FORMAT.STATIC
CSVDYLPA.
CSVDYLPA.ADD.
CSVDYLPA.ADD.
CSVDYNEX.
CSVDYNEX.LIST
CSVDYNL.
CSVDYNL.UPDATE.LNKLST
CSVLLA.

If DEFPROT is specified in the IBMFAC RDT the following command examples are not required. To prevent access to these resources, the CSV resources are protected using the following commands.

The following commands are provided for example only:

TSS ADDTO(deptacid) IBMFAC(CSV)
or
TSS ADDTO(deptacid) IBMFAC(CSVAPF)
TSS ADDTO(deptacid) IBMFAC(CSVDYLPA)
TSS ADDTO(deptacid) IBMFAC(CSVDYNEX)
TSS ADDTO(deptacid) IBMFAC(CSVDYNL)
TSS ADDTO(deptacid) IBMFAC(CSVDYLPA)
TSS ADDTO(deptacid) IBMFAC(CSVLLA)

Limit authority to those resources to z/OS systems programmers. Restrict to the absolute minimum number of personnel with ACTION(AUDIT) and UPDATE access.

Sample commands are shown here to accomplish this:

TSS PERMIT(syspsmpl) IBMFAC(CSVAPF.) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(syspsmpl) IBMFAC(CSVAPF.MVS.SETPROG) ACCESS(UPDATE)
ACTION(AUDIT)
TSS PERMIT(syspsmpl) IBMFAC(CSVAPF.MVS.SETPROG.FORMAT) ACCESS(UPDATE)
ACTION(AUDIT)
TSS PERMIT(syspsmpl)
IBMFAC(CSVAPF.MVS.SETPROG.SETPROG.FORMAT.DYNAMIC) ACCESS(UPDATE)
ACTION(AUDIT)
TSS PERMIT(syspsmpl) IBMFAC(CSVAPF.MVS.SETPROG.SETPROG.FORMAT.STATIC)
ACCESS(UPDATE) ACTION(AUDIT)

The CSVDYLPA.ADD resource will be permitted to BMC Mainview, CA 1, and CA Common Services STC ACIDs with ACTION(AUDIT) and UPDATE access.

The CSVDYLPA resource will be permitted to BMC Mainview, CA 1, and CA Common Services STC ACIDs with ACTION(AUDIT) and UPDATE access.

Sample commands are shown here to accomplish one set of resources:

TSS PERMIT(syspsmpl) IBMFAC(CSVDYLPA.) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(BMC Mainview STC ACID) IBMFAC(CSVDYLPA.ADD.) ACCESS(UPDATE)
ACTION(AUDIT)
TSS PERMIT(CA 1 STC ACID) IBMFAC(CSVDYLPA.ADD.) ACCESS(UPDATE)
ACTION(AUDIT)
TSS PERMIT(CCS STC ACID) IBMFAC(CSVDYLPA.ADD.) ACCESS(UPDATE)
ACTION(AUDIT)
TSS PERMIT(CA 1 STC ACID) IBMFAC(CSVDYLPA.DELETE.) ACCESS(UPDATE)
ACTION(AUDIT)
TSS PERMIT(CCS STC ACID) IBMFAC(CSVDYLPA.DELETE.) ACCESS(UPDATE)
ACTION(AUDIT)

The CSVDYNEX.LIST resource and/or generic equivalent will be defined with ACTION(AUDIT) and UPDATE access restricted to system programming personnel.

The CSVDYNEX.LIST resource and/or generic equivalent will be defined with READ access restricted to auditors.

Sample commands are shown here to accomplish this:

TSS PERMIT(syspsmpl) IBMFAC(CSVDYNEX.) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(syspsmpl) IBMFAC(CSVDYNEX.LIST) ACCESS(UPDATE)
ACTION(AUDIT)
TSS PERMIT(smplsmpl) IBMFAC(CSVDYNEX.LIST) ACCESS(READ)

The CSVLLA resource will be permitted to CICS and CONTROL-O STC ACIDs with

ACTION(AUDIT) and UPDATE access.

Sample commands are shown here to accomplish one set of resources:

TSS PERMIT(syspsmpl) IBMFAC(CSVLLA.) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(CICS STC ACIDs) IBMFAC(CSVLLA.) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(CONTROL-O STC ACID) IBMFAC(CSVLLA.) ACCESS(UPDATE) ACTION(AUDIT)

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223918
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223918r877759_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000450
Rule Title: IBM z/OS system commands must be properly protected.
Legacy ID: V-98543
Legacy ID: SV-107647

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
From a command screen enter:

TSS WHOHAS OPERCMDS(MVS)

If any of below is untrue for any z/OS system command resource, this is a finding.

Access to MVS resource of the OPERCMDS class is restricted to a limited number of authorized users, and all access logged.
Access to "MVS.**" is not allowed.

Access to z/OS system commands as defined in the table entitled MVS commands, RACF access authorities, and resource names, in the IBM z/OS MVS System Commands manual, is restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users).

NOTE: Use the GROUP category specified in the table referenced above as a guideline to determine appropriate personnel access to system commands.

NOTE: The (MVS.SEND) Command will not be a finding if used by all.

Access to specific z/OS system commands is logged as indicated in the table entitled MVS commands, RACF access authorities, and resource names, in the IBM z/OS MVS System Commands manual.

Fix Text: Ensure access to the MVS resource of the OPERCMDS class is restricted to a limited number of authorized users, and all access is logged. Ensure access to z/OS system commands as defined in the table entitled MVS commands, RACF access authorities, and resource names, in the IBM z/OS MVS System Commands manual is restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users).

Ensure no access is granted at level MVS.**.
NOTE: Use the GROUP category specified in the table referenced above as a guideline to determine appropriate personnel access to system commands.
NOTE: The (MVS.SEND) Command will not be a finding if used by all.

Example:
TSS ADDTO(deptacid) OPERCMDS(MVS.)
TSS PERMIT(usracid) OPERCMDS(MVS.ACTIVATE) ACTION(AUDIT)
TSS PERMIT(usracid) OPERCMDS(MVS.CANCEL.JOB.) ACTION(AUDIT)
TSS PERMIT(usracid) OPERCMDS(MVS.CONTROL.) ACCESS(UPDATE)
ACTION(AUDIT)
TSS PERMIT(usracid) OPERCMDS(MVS.DISPLAY.) ACCESS(READ)
TSS PERMIT(usracid) OPERCMDS(MVS.MONITOR) ACCESS(READ)
TSS PERMIT(usracid) OPERCMDS(MVS.STOPMN) ACCESS(READ)

CCI: CCI-000213

Group ID (Vulid): V-223919
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223919r877760_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000460
Rule Title: IBM z/OS MCS consoles access authorization(s) for CONSOLE resource(s) must be properly protected.
Legacy ID: V-98545
Legacy ID: SV-107649

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000324-GPOS-00125

Check Content:
From the ISPF Command Shell enter:
TSS WHOOWNS SYSCONS(*)

For each Console defined enter:
TSS WHOHAS SYSCONS(<console>)

If the ACID associated with each console has READ access to the corresponding resource defined in the SYSCONS resource class, this is not a finding.

If access authorization for SYSCONS resources restricts access to operations, the Master SCA, system programming personnel, or authorized personnel, this is not a finding.

If the console defined is not defined to the TSS SYSCONS resource class enter:

TSS LIST (RDT) RESCLASS(SYSCONS)

If the SYSCONS resource class does not have the DEPROT attribute, this is a finding.

For each Console defined enter:
TSS WHOHAS(<CONSOLE>)

If the console defined is not defined to the TSS SYSCONS resource class enter:
TSS LIST (RDT) RESCLASS(SYSCONS)

If the SYSCONS resource class does not have the DEPROT attribute, this is a finding.

Fix Text: Ensure that all MCS consoles are defined to the SYSCONS resource class and READ access is limited to operators, and system programmers, or authorized personnel.

Review the MCS console resources defined to z/OS and the ACP and ensure they conform to those outlined below.

Each console defined in the CONSOLxx parmlib members is defined to TSS SYSCONS resource class and/or the SYSCONS resource class has the DEFPROT attribute.

Example:

TSS REPLACE(RDT) RESCLASS(SYSCONS) ATTR(DEFPROT)

The ACID associated with each console has access to the corresponding resource defined in the SYSCONS resource class.

Example:

TSS PERMIT(MMGMST) SYSCONS(MMGMST) ACCESS(READ)

Access authorization for SYSCONS resources restricts access to operations, the Master SCA, and system programming personnel.

TSS PERMIT(opersmpl) SYSCONS(MMGMST) ACCESS(READ)
TSS PERMIT(Master SCA) SYSCONS(MMGMST) ACCESS(READ)
TSS PERMIT(syspsmpl) SYSCONS(MMGMST) ACCESS(READ)

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223920
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223920r877761_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000470
Rule Title: CA-TSS must properly define users that have access to the CONSOLE resource in the TSOAUTH resource class.
Legacy ID: V-98547
Legacy ID: SV-107651

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
TSS WHOOWNS TSOAUTH(*)
If the Console is not defined to TSOAuth RESOURCE CLASS this is Not Applicable.

Refer to the CONSOLxx member of SYS1.PARMLIB.

For each Console defined if the following is true, this is not a finding.

-User ACIDs are restricted to the INFO level in the MCSAUTH attribute.
-User ACIDs are restricted to READ access to the MVS.MCSOPER.acid resource defined in the OPERCMDS resource class.
-User ACIDs and/or profile ACIDs are restricted to the CONSOLE resource defined in the TSOAUTH resource class.

If any of the above are untrue, this is a finding.

Fix Text: Evaluate the impact of correcting any deficiencies. Develop a plan of action and implement the required changes.

At the discretion of the ISSO, users may be allowed to issue z/OS system commands from a TSO session. With this in mind, ensure the following items are in effect for users granted the TSO CONSOLE privilege:
-User ACIDs are restricted to the INFO level in the MCSAUTH attribute.
-User ACIDs are restricted to READ access to the MVS.MCSOPER.acid resource defined in the OPERCMDS resource class.
-User ACIDs and/or profile ACIDs are restricted to the CONSOLE resource defined in the TSOAUTH resource class.

For Example:
TSS ADDTO (userid) MCSAUTH(INFO)
TSS PERMIT(userid) OPERCMDS(MVS.MCSOPER.userid)
ACCESS(READ) ACTION(AUDIT)
TSS PERMIT(oprprofileacid) TSOAUTH(CONSOLE)
ACCESS(READ) ACTION(AUDIT)

CCI: CCI-000213

Group ID (Vulid): V-223921
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223921r877762_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000480
Rule Title: IBM z/OS Operating system commands (MVS.) of the OPERCMDS resource class must be properly owned.
Legacy ID: V-98549
Legacy ID: SV-107653

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices,

files, records, processes, programs, and domains) in the information system.

Check Content:
From the ISPF Command Shell enter:
TSS WHOOWNS OPERCMDS(MVS)

If the (MVS) resource is owned, this is not a finding.

If the (MVS) resource is not owned, this is a finding.

TSS LIST RDT RESCLASS(OPERCMDS)

If the (MVS) resource is not OWNED and the OPERCMDS class does not have DEFPROT as an attribute, this is a finding.

Fix Text: z/OS system command controls are provided via resources in the OPERCMDS resource class. Configure (MVS) of the OPERCMDS resource class to be properly owned or at a minimum the OPERCMDS resource in the RDT specifies the DEFPROT attribute. Name the actual owning ACID specified for deptacid in accordance with installation recommendations.

When protecting the facilities for z/OS system commands via the OPERCMDS class, use the following controls:

(1) Prevent access to the z/OS resources by default, and log all access. Create generic and specific permissions with logging as required using the required controls for z/OS System Commands listed in ACP00282.

For example:

TSS ADDTO(deptacid) OPERCMDS(MVS.)
TSS PERMIT(usracid) OPERCMDS(MVS.ACTIVATE) ACTION(AUDIT)
TSS PERMIT(usracid) OPERCMDS(MVS.CANCEL.JOB.) ACTION(AUDIT)
TSS PERMIT(usracid) OPERCMDS(MVS.CONTROL.) ACCESS(UPDATE)
ACTION(AUDIT)
TSS PERMIT(usracid) OPERCMDS(MVS.DISPLAY.) ACCESS(READ)
TSS PERMIT(usracid) OPERCMDS(MVS.MONITOR) ACCESS(READ)
TSS PERMIT(usracid) OPERCMDS(MVS.STOPMN) ACCESS(READ)

CCI: CCI-000213

Group ID (Vulid): V-223922
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223922r877763_rule

Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000490
Rule Title: CA-TSS AUTH Control Option values specified must be set to (OVERRIDE,ALLOVER) or (MERGE,ALLOVER).
Legacy ID: V-98551
Legacy ID: SV-107655

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
TSS MODIFY STATUS

If the AUTH Control Option values are not set to AUTH(OVERRIDE, ALLOVER) or AUTH(MERGE, ALLOVER), this is a finding.

Fix Text: Configure the AUTH control option is set to (OVERRIDE, ALLOVER) or (MERGE, ALLOVER). With (OVERRIDE, ALLOVER), TSS separately searches first the user, then profiles, and then the ALL record for its access authorization. With (MERGE, ALLOVER), TSS merges and searches the user and all profiles, and then the ALL record for its access authorization. Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting to AUTH(OVERRIDE, ALLOVER) or AUTH(MERGE, ALLOVER) and proceed with the change.

CCI: CCI-000213

Group ID (Vulid): V-223923
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223923r877764_rule

Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000500
Rule Title: Access to the CA-TSS MODE resource class must be appropriate.
Legacy ID: V-98553
Legacy ID: SV-107657

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
From the ISPF Command Shell enter:
TSS WHOHAS MODE(*)

If any ACIDs is permitted a mode of "DORM", "WARN", or "IMPL", this is a finding.

Fix Text: Evaluate the impact associated with implementation of the removal of this access. Develop a plan of action to ensure that the ACIDs use the default MODE settings and proceed with the change.

CCI: CCI-000213

Group ID (Vulid): V-223924
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223924r877765_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000505
Rule Title: Data set masking characters must be properly defined to the CA-TSS security database.
Legacy ID: V-98555

Legacy ID: SV-107659

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
From the ISPF Command Shell enter:
TSS WHOOWNS data set(*)

If data set masking characters. (*, %, and +, **) are owned by the MSCA, this is not a finding.

Fix Text: Configure all data set masking characters to be owned the MSCA.

Example TSS commands to protect masking characters:

TSS ADD(msca) DSN(*)
TSS ADD(msca) DSN(%)
TSS ADD(msca) DSN(+)

CCI: CCI-000213

Group ID (Vulid): V-223925
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223925r877766_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000510
Rule Title: CA-TSS Emergency ACIDs must be properly limited and must audit all resource access.
Legacy ID: SV-107661

Legacy ID: V-98557

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
Refer to the SYS1.UADS.

Ask the System Administrator for list of all emergency ACIDs available to the site along with the associated function of each.

If there are no emergency ACIDs defined ask the system administrator for an alternate documented procedure to handle emergencies.

If there are no emergency ACIDs and no documented emergency procedure, this is a finding.

If at a minimum, an emergency ACID exists with the security administration attributes specified in accordance with the following requirements, this is not a finding.

For emergency IDs with security administration privileges, but which cannot access and update system data sets:

ADMIN Authority:
ACID(ALL)
DATA(ALL)
OTRAN(ALL)
MISC1(INSTDATA,SUSPEND,TSSSIM,NOATS)
MISC2(TSO,TARGET)
MISC8(PWMAINT,REMASUSP)
MISC9(GENERIC) FACILITY(BATCH, TSO, ROSCOE, CICS, xxxx)
Where 'xxxx' is a facility the application security team grants access into for their application

users.

An additional class of userids can exist to perform all operating system functions except ESM administration.

These emergency ACID(s) will have ability to access and update all system data sets but will not have security administration privileges. See the following requirements:

Data set permissions for the emergency ACIDs will be permitted as follows:

TSS PER(acid) DSN(*****) ACCESS(ALL) ACTION(AUDIT)

Security Bypass Attributes NODSNCHK, NOVOLCHK, and NORESCHK will not be given to the Emergency ACIDs.

All emergency ACID(s) are to be implemented with logging to provide an audit trail of their activities.

All emergency ACID(s) are to be maintained in both the ESM and SYS1.UADS to ensure they are available in the event that the ESM is not functional.

All emergency ACID(s) will have distinct, different passwords in SYS1.UADS and in the ACP, and the site is to establish procedures to ensure that the passwords differ. The password for any ID in SYS1.UADS is never to match the password for the same ID in the ACP.

All emergency ACID(s) will have documented procedures to provide a mechanism for the use of the IDs. Their release for use is to be logged, and the log is to be maintained by the ISSO. When an emergency ACID is released for use, its password is to be reset by the ISSO within 12 hours.

1) Review the access authorizations for all emergency ACIDs to ensure that all access permitted to these ACIDs is reviewed and approved by the ISSO.
2) If emergency ACIDs are utilized, ensure they are restricted to performing only the operating system recovery functions or the ESM administration functions.

If these emergency ACID(s) have ability to ACCESS and UPDATE all system data sets, but do not have security administration privileges, this is not a finding.

Note: If running Quest NC-Pass, validate that the Emergency ACIDS are identified to have the FACILITY of NCPASS and SECURID resource in the ABSTRACT resource class.

Fix Text: Configure any emergency ACID to have only access to resources required to support the specific functions of the owning department and that access to these resources is audited. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes.

TSS PER(acid) DSN(*****) ACCESS(ALL) ACTION(AUDIT)

Security Bypass Attributes NODSNCHK, NOVOLCHK, and NORESCHK will not be given to the Emergency ACIDs.

All emergency ACID(s) are to be implemented with logging to provide an audit trail of their activities.

All emergency ACID(s) are to be maintained in both the ACP and SYS1.UADS to ensure they are available in the event that the ACP is not functional.

All emergency ACID(s) will have distinct, different passwords in SYS1.UADS and in the ACP, and the site is to establish procedures to ensure that the passwords differ. The password for any ID in SYS1.UADS is never to match the password for the same ID in the ACP.

All emergency ACID(s) will have documented procedures to provide a mechanism for the use of the IDs. Their release for use is to be logged, and the log is to be maintained by the ISSO. When an emergency ACID is released for use, its password is to be reset by the ISSO within 12 hours.

If no emergency userids are in use on the system, develop and document a procedure to manage emergency access to the system.

CCI: CCI-000213

Group ID (Vulid): V-223926
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223926r877767_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000520
Rule Title: CA-TSS ACIDs must not have access to FAC(*ALL*).
Legacy ID: SV-107663
Legacy ID: V-98559

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
From the ISPF Command Shell enter:
TSS LIST(ACIDS) DATA(BASIC)

If any ACID(s) is (are) assigned FACILITY(*ALL*), this is a finding.

Fix Text: The ISSO will ensure that blanket access to all facilities; FACILITY(ALL), is never granted.

Review all access to FACILITY(*ALL*). Evaluate the impact of correcting the deficiency. Develop a plan of action and remove access to FAC(*ALL*).

Example:
TSS REM(acid) FAC(ALL)

CCI: CCI-000213

Group ID (Vulid): V-223927
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223927r877768_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000530
Rule Title: The CA-TSS ALL record must have appropriate access to Facility Matrix Tables.
Legacy ID: SV-107665
Legacy ID: V-98561

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
Review the ALL record for the assignment of FACILITY.

If CA-Top Secret facilities are granted via the ALL record, with the exception of DFHSM/HSM, this is a finding.

The DFHSM/HSM FACILITY can be determined by reviewing FACLIST for the FACILITY that contains INITPGM=ARC.

Fix Text: Review ALL record for FACILITY access. Evaluate the impact of correcting the deficiency. Develop a plan of action and remove access.

CCI: CCI-000213

Group ID (Vulid): V-223928
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223928r877769_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000550
Rule Title: Data set masking characters allowing access to all data sets must be properly restricted in the CA-TSS security database.
Legacy ID: V-98563
Legacy ID: SV-107667

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices,

and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
Refer the accesses to the TSS masking character (*, *., and/or **) for data sets.

If the following guidance is true, this is not a finding.

If the TSS data set access authorizations restrict READ access to auditors, this is not a finding.

If the TSS data set access authorizations restrict READ and/or greater access to DASD administrators, Trusted Started Tasks, emergency users, and DASD batch users, this is not a finding.

If CA VTAPE is installed on the systems and the TSS data set access authorizations restrict READ access to CA VTAPE STCs and/or batch users, this is not a finding.

If the TSS data set access authorizations specify that all (i.e., failures and successes) EXECUTE and/or greater accesses are logged, this is not a finding.

Fix Text: Review access authorization to the TSS mask character (*, *., and/or **) for data sets. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to restrict access to the data set mask permissions.

The installing Systems Programmer will identify and document the product data sets and categorize them according to who will have WRITE and/or greater access and, if required, that all WRITE and/or greater accesses are logged. The programmer will identify if any additional groups have WRITE and/or greater access for specific data sets, and once documented, will work with the ISSO to confirm that they are properly restricted to the ACP (Access Control Program) active on the system.

(Note: The data sets and/or data set prefixes identified below are examples of a possible installation. The actual data sets and/or prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.)

Auditors may require READ access to all data sets.
DASD administrators, Trusted Started Tasks, emergency users, and DASD batch users that require READ and/or greater access to perform maintenance to all data sets.
If CA VTAPE is installed on the system, READ access can be given to the CA VTAPE STCs and/or batch users.
All accesses authorizations will be logged. The exception is the logging requirement is not required for Trusted Started Tasks.

The following commands are provided as a sample for implementing data set controls:

TSS ADDTO(msca) DATASET(*.)
TSS PERMIT(smplsmpl) DATASET(*.) ACCESS(READ) ACTION(AUDIT)
TSS PERMIT(CA VTape STC) DATASET(*.) ACCESS(READ) ACTION(AUDIT)
TSS PERMIT(dasbsmpl) DATASET(*.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(dasdsmpl) DATASET(*.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(emersmpl) DATASET(*.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(tstcsmpl) DATASET(*.) ACCESS(ALL)

CCI: CCI-000213

Group ID (Vulid): V-223929
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223929r877770_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000560
Rule Title: IBM z/OS DASD Volume access greater than CREATE found in the CA-TSS database must be limited to authorized information technology personnel requiring access to perform their job duties.
Legacy ID: V-98565
Legacy ID: SV-107669

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
From the ISPF Command Shell enter:
TSS WHOOWNS VOLUME(*)

For each volume identified issue WHOHAS (<volume id>)

If access authorizations greater than CREATE (e.g., CONTROL or ALL) granted for DASD volumes are within the requirements in the site security plan, this is not a finding.

If access authorization for volumes exceeds the requirements without justification, this is a finding.

NOTE: Domain-level DASD Administrators who are responsible for the Domain level DASD/storage administration. Volume level access to those team members who are directly responsible and perform Domain level DASD/Storage administration may be granted access to all volumes via PRIVPGM controls.

Fix Text: Ensure that DASD VOLUME access authorization greater than CREATE is not permitted unless authorized by the ISSO.

Review all access to DASD VOLUMEs. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the required changes.

*Noted Exception: Domain level DASD Administrators who are responsible for the Domain level DASD/storage administration. Volume level access to those team members who are directly responsible and perform Domain level DASD/Storage administration may be granted access to all volumes via PRIVPGM controls.

Domain Level DASD/Storage administrators access should be granted VOL(*ALL*)ACC(ALL)ACTION(AUDIT)PRIVPGM(list of privileged programs)

CCI: CCI-000213

Group ID (Vulid): V-223930
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223930r877771_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000570
Rule Title: IBM z/OS Sensitive Utility Controls must be properly defined and protected.
Legacy ID: SV-107671
Legacy ID: V-98567

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures

and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
Refer to the table of Sensitive Utilities resources and/or generic equivalent as detail in the table below.

If the TSS resource access authorizations for the following sensitive utilities restrict access to the appropriate personnel, this is not a finding.

Sensitive Utility Controls
Program Product Function
AHLGTF z/OS System Activity Tracing
HHLGTF
IHLGTF

ICPIOCP z/OS System Configuration
IOPIOCP
IXPIOCP
IYPIOCP
IZPIOCP

BLSROPTR z/OS Data Management

DEBE OS/DEBE Data Management

DITTO OS/DITTO Data Management

FDRZAPOP FDR Product Internal Modification

GIMSMP SMP/E Change Management Product

ICKDSF z/OS DASD Management

IDCSC01 z/OS IDCAMS Set Cache Module

IEHINITT z/OS Tape Management

IFASMFDP z/OS SMF Data Dump Utility

IND$FILE z/OS PC to Mainframe File Transfer
(Applicable only for classified systems)

CSQJU003 IBM WebSphereMQ
CSQJU004
CSQUCVX
CSQ1LOGP
CSQUTIL

WHOIS z/OS Share MOD to identify user name from USERID.
Restricted to data center personnel only.

If the TSS resources are owned or DEFPROT is specified for the resource class, this is not a finding.

If the TSS resource logging is correctly specified, this is not a finding.

Fix Text: Ensure that the following are properly specified in the ACP.

Note: The resources and/or resource prefixes identified below are examples of a possible installation. The actual resource type, resources, and/or resource prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.

Ensure that all Sensitive Utility Controls resources and/or generic equivalent are properly protected according to the requirements specified in Sensitive Utility Controls table below. This table lists the resources, access requirements, and logging requirements for Sensitive Utilities, ensures the following guidelines are followed:

Sensitive Utility Controls
Program Product Function
AHLGTF z/OS System Activity Tracing
HHLGTF
IHLGTF

ICPIOCP z/OS System Configuration
IOPIOCP
IXPIOCP
IYPIOCP
IZPIOCP

BLSROPTR z/OS Data Management

DEBE OS/DEBE Data Management

DITTO OS/DITTO Data Management

FDRZAPOP FDR Product Internal Modification

GIMSMP SMP/E Change Management Product

ICKDSF z/OS DASD Management

IDCSC01 z/OS IDCAMS Set Cache Module

IEHINITT z/OS Tape Management

IFASMFDP z/OS SMF Data Dump Utility

IND$FILE z/OS PC to Mainframe File Transfer
(Applicable only for classified systems)

CSQJU003 IBM WebSphereMQ
CSQJU004
CSQUCVX
CSQ1LOGP
CSQUTIL

WHOIS z/OS Share MOD to identify user name from USERID.
Restricted to data center personnel only.

The TSS resources as designated in the above table are owned and/or DEFPROT is specified for the resource class.

The TSS resource access authorizations restrict access to the appropriate personnel as designated in the above table.

The following commands are provided as a sample for implementing resource controls:

TSS ADD(dept-acid) PROGRAM(AHLGTF)
TSS PERMIT(stcgsmpl) PROGRAM(AHLGTF) ACTION(AUDIT)

CCI: CCI-000213

Group ID (Vulid): V-223931
Group Title: SRG-OS-000480-GPOS-00229
Rule ID: SV-223931r881331_rule

Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000580
Rule Title: IBM z/OS Started tasks must be properly defined to CA-TSS.
Legacy ID: V-98569
Legacy ID: SV-107673

Vulnerability Discussion: Started procedures have system generated job statements that do not contain the user, group, or password statements. To enable the started procedure to access the same protected resources that users and groups access, started procedures must have an associated USERID. If a USERID is not associated with the started procedure, the started procedure will not have access to the resources.

To ensure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Check Content:
Refer to the site security plan, the system administrator, and system libraries to determine list of stated tasks available on the system.

If the following guidance is true, this is not a finding.

-All started tasks are assigned a unique user ACID or STC ACIDs that will be unique per product and function if supported by vendor documentation.

-Every ACID with the STC Facility has a corresponding entry defined in the STC record.

-Every ACID defined in the STC record has a corresponding user ACID defined to TSS with the STC Facility.

-All STC ACIDs will have a password generated in accordance with STIG requirements.

-All STC ACIDs will be sourced to the internal reader (e.g., ADD(stc-acid) SOURCE(INTRDR).

-The STC ACIDs may have the NOSUSPEND attribute.

Fix Text: Review the STC record and all associated ACIDs. Ensure STCs and associated ACIDs are defined to the STC record. Restrict access to required resources only. Evaluate the impact of correcting the deficiency. Ensure TSS started task table record contains an entry for each Started Proc that maps the proc to a unique userid, or STC ACIDs will be unique per product and function if supported by vendor documentation. Develop a plan of action and implement the changes as specified:

All STC ACIDs will have the STC facility. An STC also may be granted the FAC(BATCH) if it requires the capability to submit batch jobs to the internal reader. It should be noted, however,

that this also will allow the STC itself to be executed as a batch job.

TSS ADD(stc-acid) FACILITY(STC BATCH)

Each STC ACID will be defined with a password following the password requirement guidelines. The only exception is that these passwords will be defined as non-expiring. In addition, each STC will have its own unique password. Defining a password for started tasks prevents a user from logging onto a system with the STC ACID.

TSS REP(stc-acid) PASSWORD(xxxxxxxx,0)

Ensure the OPTIONS control option specifies a value of 4 to disable password checking for STCs. Otherwise operators will be forced to supply a password when STCs are started.

All STC ACIDs will be sourced to the internal reader. This control will further protect the unauthorized use of STC ACIDs.

TSS ADD(stc-acid) SOURCE(INTRDR)

Every STC will be defined to the STC table, associated with a specific procedure, and granted minimum access.

TSS ADD(STC) PROCNAME(stc-proc) ACID(stc-acid)

Note: The STC ACIDs may have the NOSUSPEND attribute to exempt an STC ACID from suspension for excessive violations. Review the STC record and all associated ACIDs. Ensure STCs and associated ACIDs are defined to the STC record. Restrict access to required resources only. Evaluate the impact of correcting the deficiency. Ensure TSS started task table record contains an entry for each Started Proc that maps the proc to a unique userid, or STC ACIDs will be unique per product and function if supported by vendor documentation. Develop a plan of action and implement the changes as specified:

All STC ACIDs will have the STC facility. An STC also may be granted the FAC(BATCH) if it requires the capability to submit batch jobs to the internal reader. It should be noted, however, that this also will allow the STC itself to be executed as a batch job.

TSS ADD(stc-acid) FACILITY(STC BATCH)

Each STC ACID will be defined with a password following the password requirement guidelines. The only exception is that these passwords will be defined as non-expiring. In addition, each STC will have its own unique password. Defining a password for started tasks prevents a user from logging onto a system with the STC ACID.

TSS REP(stc-acid) PASSWORD(xxxxxxxx,0)

Ensure the OPTIONS control option specifies a value of 4 to disable password checking for

STCs. Otherwise operators will be forced to supply a password when STCs are started.

All STC ACIDs will be sourced to the internal reader. This control will further protect the unauthorized use of STC ACIDs.

TSS ADD(stc-acid) SOURCE(INTRDR)

Every STC will be defined to the STC table, associated with a specific procedure, and granted minimum access.

TSS ADD(STC) PROCNAME(stc-proc) ACID(stc-acid)

Note: The STC ACIDs may have the NOSUSPEND attribute to exempt an STC ACID from suspension for excessive violations.

CCI: CCI-000366

Group ID (Vulid): V-223932
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223932r877773_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000590
Rule Title: The CA-TSS CANCEL Control Option must not be specified.
Legacy ID: V-98571
Legacy ID: SV-107675

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

The CANCEL Control Option allows security administrators to use the O/S CANCEL command to bring the TSS address space down.

Check Content:
From the ISPF Command enter:
TSS MODIFY STATUS

If the CANCEL Control Option is not specified, this is not a finding.

Fix Text: Remove the CANCEL sub-option from the Control Options list.

TSS MODIFY(control_option [(suboption_list)])

CCI: CCI-000366

Group ID (Vulid): V-223933
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223933r877774_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000600
Rule Title: The CA-TSS HPBPW Control Option must be set to three days maximum.
Legacy ID: SV-107677
Legacy ID: V-98573

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Check Content:
From the ISPF Command enter:
TSS MODIFY STATUS

If the HPBPW Control Option value is set to (3) days maximum, this is not a finding.

If the HPBPW Control Option value is set to greater than (3) days, this is a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the HPBPW control option setting to a maximum of 3 days.

CCI: CCI-000366

Group ID (Vulid): V-223934

Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223934r877775_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000610
Rule Title: The CA-TSS INSTDATA Control Option must be set to 0.
Legacy ID: SV-107679
Legacy ID: V-98575

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Check Content:
From the ISPF Command enter:
TSS MODIFY STATUS

If the INSTDATA Control Option is set to NONE this is not a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to set the INSTDATA control option value to (0) and proceed with the change.

CCI: CCI-000366

Group ID (Vulid): V-223935
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223935r877776_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000620
Rule Title: The CA-TSS OPTIONS Control Option must include option 4 at a minimum.
Legacy ID: SV-107681
Legacy ID: V-98577

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Check Content:
From the ISPF Command Shell enter:

TSS MODIFY STATUS

If the OPTIONS Control Option contains at a minimum option number (4), this is not a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting as specified following and proceed with the change.

The OPTIONS Control Option must contain at a minimum option number (4).

Example TSS PARMFILE Control Option entry:
OPTIONS(4,5,6,12,14)

CCI: CCI-000366

Group ID (Vulid): V-223936
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223936r877777_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000630
Rule Title: CA-TSS TEMPDS Control Option must be set to YES.
Legacy ID: SV-107683
Legacy ID: V-98579

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the TEMPDS Control Option value is set to TEMPDS(YES), this not a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting to TEMPDS(YES), and proceed with the change.

CCI: CCI-000366

Group ID (Vulid): V-223937
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223937r877778_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000640
Rule Title: The number of CA-TSS control ACIDs must be justified and properly assigned.
Legacy ID: SV-107685
Legacy ID: V-98581

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Check Content:
From the ISPF Command Shell enter:
TSS LIST(ACIDS) TYPE(SCA) DATA(BASIC)

If the persons listed agree with the site security plan, this is not a finding.

Fix Text: Review all security administrator ACIDs. Evaluate the impact of correcting the deficiency. Develop a plan of action and reduce the number of control ACIDs if not justified. Use information below as guidance.

TYPE=CENTRAL, TYPE=MASTER or also known as "SCA" and "MSCA" level of ACIDS will adhere to the following restrictions based upon documented role/function an individual performs:

-Domain level Information System Security Officer (ISSO) - full administrative authorities and access rights needed to perform required and documented role/responsibilities/function.
-Assistance Domain Level Information System Security Officer or "backup" or ISSO (up to same access as 1).
-DISA SRR Auditor, DoD IG Auditor, SAS70 Auditor - only "view" administrative authorities must be granted and only for those roles/functions that have been formally documented as DISA,

DoD IG or SAS70 Auditors and approved by the DISA AO for those position/functions/roles.

Exception: Until scoping is worked out and resolved, DISA OST team members may be defined as TYPE=CENTRAL with limited authority such as ACID(INFO,MAINTAIN). All OST Team member ACIDs will be changed to TYPE=LIMITED and scoped accordingly to allow password resets upon verification of users, yet to limit and eliminate any potential risk associated with resetting of MSCA or other SCA level accounts. NO other exceptions will exist.

CCI: CCI-000366

CCI: CCI-002145

Group ID (Vulid): V-223938
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223938r877779_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000650
Rule Title: The number of CA-TSS ACIDs with MISC9 authority must be justified.
Legacy ID: SV-107687
Legacy ID: V-98583

Vulnerability Discussion: Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Check Content:
From the ISPF Command Shell enter:
TSS LIST(ACIDS) DATA(ADMIN)

If the ACIDs having MISC9(ALL) or MISC9(CONSOLE) authority are designated SCAs who are responsible for the security for the domain this is not a finding.

Fix Text: Review all ACIDs with the MISC9 attribute. Evaluate the impact of removing MISC9(ALL) or MISC9(CONSOLE) access from ACIDs not required to assign the CONSOLE attribute. It is suggested that MISC9(CONSOLE) assignment privileges be limited to the MSCA. Develop a plan of action and implement the changes.

CCI: CCI-000366

CCI: CCI-002145

Group ID (Vulid): V-223939
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223939r877780_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000660
Rule Title: The CA-TSS LUUPDONCE Control Option value specified must be set to NO.
Legacy ID: SV-107689
Legacy ID: V-98585

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the LUUPDONCE Control Option value is set to "YES", this is a finding.

Fix Text: Configure LUUPDONCE control option is set to (NO). Evaluate the impact associated with implementation of the control option. Develop a plan of action to set the control option setting to NO and proceed with the change.

CCI: CCI-000366

CCI: CCI-002251

Group ID (Vulid): V-223940
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223940r877781_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000670
Rule Title: The CA-TSS Automatic Data Set Protection (ADSP) Control Option must be set to NO.
Legacy ID: V-98587
Legacy ID: SV-107691

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the ADSP Control Option value is not set to "ADSP(NO)", this is a finding.

Fix Text: Configure the ADSP control option is set to (NO) indicating that the RACF bit in the DSCB will not be set. Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting to ADSP(NO) and proceed with the change.

CCI: CCI-000366

CCI: CCI-002358

Group ID (Vulid): V-223941

Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223941r877782_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000680
Rule Title: CA-TSS RECOVER Control Option must be set to ON.
Legacy ID: V-98589
Legacy ID: SV-107693

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the RECOVER Control Option value is not set to "RECOVER(ON)", this is a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the following control option setting as specified and proceed with the change.

RECOVER(ON)

CCI: CCI-000366

CCI: CCI-000550

Group ID (Vulid): V-223942
Group Title: SRG-OS-000096-GPOS-00050
Rule ID: SV-223942r877783_rule
Severity: CAT II

Rule Version (STIG-ID): TSS0-ES-000690
Rule Title: IBM z/OS must properly configure CONSOLxx members.
Legacy ID: V-98591
Legacy ID: SV-107695

Vulnerability Discussion: In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., VPN and IPS); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the operating system must support the organizational requirements, providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

Check Content:
Review each CONSOLxx parmlib member.

If the following guidance is true, this is not a finding.

The "DEFAULT" statement for each CONSOLxx member specifies "LOGON(REQUIRED)" or "LOGON(AUTO)".

The "CONSOLE" statement for each console assigns a unique name using the "NAME" parameter.

The "CONSOLE" statement for each console specifies "AUTH(INFO)". Exceptions are the "AUTH" parameter is not valid for consoles defined with "UNIT(PRT)" and specifying "AUTH(MASTER)" is permissible for the system console.

Note: The site should be able to determine the system consoles. However, it is imperative that the site adhere to the "DEFAULT" statement requirement.

Fix Text: Configure the "DEFAULT" statement to specify "LOGON(REQUIRED)" so that all operators are required to log on prior to entering z/OS system commands. At the discretion of the ISSO, "LOGON(AUTO)" may be used. If "LOGON(AUTO)" is used assure that the console userids are defined with minimal access. See ACP00292.

Configure each "CONSOLE" statement to specify an explicit console NAME. And that "AUTH(INFO)" is specified, this also including extended MCS consoles. "AUTH(MASTER)" may be specified for systems console.

Note: The site should be able to determine the system consoles. However, it is imperative that the site adhere to the "DEFAULT" statement requirement.

CCI: CCI-000382

Group ID (Vulid): V-223943
Group Title: SRG-OS-000096-GPOS-00050
Rule ID: SV-223943r877784_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000700
Rule Title: IBM z/OS must properly protect MCS console userid(s).
Legacy ID: V-98593
Legacy ID: SV-107697

Vulnerability Discussion: In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., VPN and IPS); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the operating system must support the organizational requirements, providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

Check Content:
Refer to IEASYS00 to determine correct CONSOLxx member.

Examine the CONSOLxx member.

If the following guidance is true, this is not a finding.

Each console defined in the currently active CONSOLxx parmlib member in

EXAM.RPT(PARMLIB) is associated with a valid TSS ACID.

Each console ACID has no special privileges and/or attributes (e.g., BYPASSING, CONSOLE, etc.; excluding VTAM SMCS consoles).

Each console ACID has no accesses to interactive on-line facilities (e.g., TSO, CICS, etc.; excluding VTAM SMCS consoles). Each console can have the Facility of CONSOLE.

Each console ACID will be restricted from accessing all data sets and resources except MVS.MCSOPER.consolename in the OPERCMDS resource class and consolename in the CONSOLE resource class.

NOTE: If LOGON(AUTO) is specified in the currently active CONSOLxx parmlib member, additional access may be required. Permissions for the console ACIDs and/or console profile may be given with access READ to MVS.CONTROL, MVS.DISPLAY, MVS.MONITOR, and MVS.STOPMN OPERCMDS resource.

Fix Text: Review the MCS console resources defined to z/OS and the ACP, and ensure they conform to those outlined below.

Each console defined in the currently active CONSOLxx parmlib member in EXAM.RPT(PARMLIB) is associated with a valid TSS ACID.

Each console ACID has no special privileges and/or attributes (e.g., BYPASSING, CONSOLE, etc.).

Each console ACID has no accesses to interactive on-line facilities (e.g., TSO, CICS, etc.; excluding VTAM SMCS consoles).

Each console can have the Facility of CONSOLE.

Each console ACID will be restricted from accessing all data sets and resources except MVS.MCSOPER.consolename in the OPERCMDS resource class and consolename in the CONSOLE resource class.

NOTE: If LOGON(AUTO) is specified in the currently active CONSOLxx parmlib member, additional access may be required. Permissions for the console ACIDs and/or console profile may be given with access READ to MVS.CONTROL, MVS.DISPLAY, MVS.MONITOR, and MVS.STOPMN OPERCMDS resource.

Example: (These are only examples, not requirements.)

TSS CREATE(consnoautolog) TYPE(PROFILE)
NAME('MCS consoles with no autolog')
DEPT('SYS1')

TSS CREATE(consautolog) TYPE(PROFILE) -
NAME('MCS consoles with autolog') -
DEPT('SYS1')

TSS CREATE(consname) NAME('MCS console name') -
FACILITY(CONSOLE) PASSWORD(password,0) -
PROFILE(consgroup)

TSS PER(consautolog) OPERCMDS(MVS.CONTROL) ACCESS(READ)
TSS PER(consautolog) OPERCMDS(MVS.DISPLAY) ACCESS(READ)
TSS PER(consautolog) OPERCMDS(MVS.MONITOR) ACCESS(READ)
TSS PER(consautolog) OPERCMDS(MVS.STOPMN) ACCESS(READ)

TSS PER(consname) SYSCONS(consname) ACCESS(READ)

CCI: CCI-000382

Group ID (Vulid): V-223944
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223944r877785_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000710
Rule Title: The CA-TSS CPFRCVUND Control Option value specified must be set to NO.
Legacy ID: V-98595
Legacy ID: SV-107699

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the "CPFRCVUND" Control Option value is set to "YES", this is a finding.

Fix Text: Configure the CPFRCVUND control option value to (NO).

Evaluate the impact associated with implementation of the control option.

Develop a plan of action to set the control option setting to "NO" and proceed with the change.

CCI: CCI-000764

Group ID (Vulid): V-223945
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223945r877786_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000720
Rule Title: The CA-TSS CPFTARGET Control Option value specified must be set to LOCAL.
Legacy ID: V-98597
Legacy ID: SV-107701

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:

From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the CPFTARGET Control Option value specified is not set to "LOCAL", this is a finding.

Fix Text: Configure the CPFTARGET Control Option value specified set to LOCAL.

CCI: CCI-000764

Group ID (Vulid): V-223946
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223946r877787_rule
Severity: CAT III
Rule Version (STIG-ID): TSS0-ES-000730
Rule Title: CA-TSS User ACIDs and Control ACIDs must have the NAME field completed.
Legacy ID: SV-107703
Legacy ID: V-98599

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
From the ISPF Command Shell enter:
TSS LIST (ACIDs) DATA (BASIC)

If any ACID does not have the "NAME" field completed, this is a finding.

Fix Text: Review all ACID definitions and ensure the NAME field is completed. Evaluate the

impact of correcting the deficiency. Develop a plan of action and implement.

CCI: CCI-000764

Group ID (Vulid): V-223947
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223947r877788_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000740
Rule Title: The CA-TSS PASSWORD(NOPW) option must not be specified for any ACID type.
Legacy ID: SV-107705
Legacy ID: V-98601

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
From the ISPF Command Shell enter:
TSS LIST(ACIDS) DATA(PASSWORD) - NOTE: To evaluate the PASSWORD option NOPW, it must be run under the MSCA's authority, if not the information will not be generated.

If PASSWORD(NOPW) is specified for any ACID types (USER, DCA, VCA, ZCA, LSCA, SCA, and MSCA), this is a finding.

Fix Text: Review definition of all ACID types (including USER, DCA, VCA, ZCA, LSCA, SCA, and MSCA) except for structure ACIDS such as: DEPARTMENT, DIVISION, ZONE, GROUP, and PROFILE to ensure that all ACIDs specify a password.

The following command is an example of how this can be corrected.

TSS REPLACE(user_ACID) PASSWORD(Text4Pwd,60

CCI: CCI-000764

Group ID (Vulid): V-223948
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223948r877789_rule
Severity: CAT III
Rule Version (STIG-ID): TSS0-ES-000750
Rule Title: Interactive ACIDs defined to CA-TSS must have the required fields completed.
Legacy ID: SV-107707
Legacy ID: V-98603

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
From the ISPF Command Shell enter:
TSS LIST (ACIDs) DATA (BASIC,TSO,CICS)

If all the fields and information listed below, are not present for all interactive users this is a finding.

FIELD DESCRIPTION VALUE
FACILITY Validated facilities to use BATCH, TSO, NCPASS, or other interactive Facility
PASSWORD logon password must have a value

INSTDATA Installation data optional
PROFILE Profile(s) optional
TSOLPROC Default TSO logon PROC optional for TSO users
TSOLACCT Default TSO logon account may be required for a fee for service.

Fix Text: Review all interactive ACID definitions to ensure required information is provided. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required according to the following:

FIELD DESCRIPTION VALUE
FACILITY Validated facilities to use BATCH, TSO, NCPASS, or other interactive Facility
PASSWORD logon password must have a value
INSTDATA Installation data optional
PROFILE Profile(s) optional
TSOLPROC Default TSO logon PROC optional for TSO users
TSOLACCT Default TSO logon account may be required
for a fee for service.

CCI: CCI-000764

Group ID (Vulid): V-223950
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223950r877791_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000770
Rule Title: CA-TSS Batch ACID(s) submitted through RJE and NJE must be sourced.
Legacy ID: SV-107711
Legacy ID: V-98607

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual

authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
Refer to data obtained from the site installation identifying batch type ACIDs.

If all static batch ACIDs (ACIDs whose passwords never change) originating from a physical reader, RJE, or NJE are sourced to those readers such as (INTRDR, N12.IR, etc.) with the appropriate source Syntax, this is not a finding.

Fix Text: Ensure that all static batch ACIDs (ACIDs whose passwords never change) originating from a physical reader, RJE, or NJE are sourced to those readers such as (INTRDR, N12.IR, etc.) with the appropriate source Syntax. Example: TSS ADD(batch-acid) SOURCE(device)

Develop a plan of action and implement the changes as specified.

CCI: CCI-000764

Group ID (Vulid): V-223951
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223951r877792_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000780
Rule Title: IBM z/OS DASD management ACIDs must be properly defined to CA-TSS.
Legacy ID: SV-107713
Legacy ID: V-98609

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts

(e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
Refer to data obtained from the site installation identifying DASD maintenance ACIDs.

If each DASD Maintenance ACID has batch Facility, this is not a finding.

Fix Text: Define all batch ACIDs to the BATCH facility.

CCI: CCI-000764

Group ID (Vulid): V-223952
Group Title: SRG-OS-000109-GPOS-00056
Rule ID: SV-223952r877793_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000790
Rule Title: CA-TSS user accounts must uniquely identify system users.
Legacy ID: V-98611
Legacy ID: SV-107715

Vulnerability Discussion: To assure individual accountability and prevent unauthorized access, organizational users must be individually identified and authenticated.

A group authenticator is a generic account used by multiple individuals. Use of a group authenticator alone does not uniquely identify individual users. Examples of the group authenticator is the UNIX OS "root" user account, the Windows "Administrator" account, the "sa" account, or a "helpdesk" account.

For example, the UNIX and Windows operating systems offer a "switch user" capability allowing users to authenticate with their individual credentials and, when needed, "switch" to the administrator role. This method provides for unique individual authentication prior to using a group authenticator.

Users (and any processes acting on behalf of users) need to be uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization, which outlines specific user actions that can be performed on the operating system without identification or authentication.

Requiring individuals to be authenticated with an individual authenticator prior to using a group authenticator allows for traceability of actions, as well as adding an additional level of protection of the actions that can be taken with group account knowledge.

Satisfies: SRG-OS-000109-GPOS-00056, SRG-OS-000121-GPOS-00062, SRG-OS-000125-GPOS-00065

Check Content:
Obtain a list of all userids that are shared among multiple users (i.e., not uniquely identified system users).

If there are no shared userids on this domain, this is not a finding.

If there are shared userids on this domain, this is a finding.

NOTE: Userid

Fix Text: Identify user accounts defined to the ESM that are being shared among multiple users. This may require interviews with appropriate system-level support personnel. Remove the shared user accounts from the ESM.

CCI: CCI-000770

CCI: CCI-000804

CCI: CCI-000877

Group ID (Vulid): V-223953
Group Title: SRG-OS-000118-GPOS-00060
Rule ID: SV-223953r877794_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000800
Rule Title: CA-TSS security administrator must develop a process to suspend userids found inactive for more than 35 days.
Legacy ID: V-98613
Legacy ID: SV-107717

Vulnerability Discussion: Inactive identifiers pose a risk to systems and applications because attackers may exploit an inactive identifier and potentially obtain undetected access to the system. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

Operating systems need to track periods of inactivity and disable application identifiers after 35 days of inactivity.

Check Content:
From the ISPF Command Shell enter:
TSS LIST(ACIDS)

If every user shows a LAST-USED=yy.ddd within the past "35" days, this is not a finding.

NOTE: VALID FOR INTERACTIVE USERIDS, NOT VALID FOR STARTED TASK USERIDS AND BATCH USERIDS.

Fix Text: Develop a procedure to check all userids for inactivity of more than "35" days. If found, the ISSO must suspend an account, but not delete it until it is verified by the local ISSO that the user no longer requires access. If verification is not received within "60" days, the account may be deleted.

CCI: CCI-000795

Group ID (Vulid): V-223954
Group Title: SRG-OS-000118-GPOS-00060
Rule ID: SV-223954r877795_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000810
Rule Title: The CA-TSS INACTIVE Control Option must be properly set.
Legacy ID: SV-107719
Legacy ID: V-98615

Vulnerability Discussion: Inactive identifiers pose a risk to systems and applications because attackers may exploit an inactive identifier and potentially obtain undetected access to the system. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

Operating systems need to track periods of inactivity and disable application identifiers after 35 days of inactivity.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the INACTIVE Control Option is set to a value of "0", this is not a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a

plan of action to set the INACTIVE Control Option to a value of "0" days and proceed with the change.

The INACTIVE Control Option value is set properly with the command:

TSS MODIFY INACTIVE(0)

CCI: CCI-000795

Group ID (Vulid): V-223955
Group Title: SRG-OS-000138-GPOS-00069
Rule ID: SV-223955r877796_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000820
Rule Title: The CA-TSS AUTOERASE Control Option must be set to ALL for all systems.
Legacy ID: SV-107721
Legacy ID: V-98617

Vulnerability Discussion: Preventing unauthorized information transfers mitigates the risk of information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

This requirement generally applies to the design of an information technology product, but it can also apply to the configuration of particular information system components that are, or use, such products. This can be verified by acceptance/validation processes in DoD or other government agencies.

There may be shared resources with configurable protections (e.g., files in storage) that may be assessed on specific information system components.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the AUTOERASE Control Option value is set to (ALL), this is not a finding.

Fix Text: Configure the AUTOERASE control option is set to (ALL) for all systems to erase all residual information on DASD. Evaluate the impact associated with implementation of the

control option. Develop a plan of action to set the AUTOERASE control option to (ALL) for all systems and implement.

CCI: CCI-001090

Group ID (Vulid): V-223956
Group Title: SRG-OS-000184-GPOS-00078
Rule ID: SV-223956r877797_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000830
Rule Title: CA-TSS DOWN Control Option values must be properly specified.
Legacy ID: V-98619
Legacy ID: SV-107723

Vulnerability Discussion: Failure to a known safe state helps prevent systems from failing to a state that may cause loss of data or unauthorized access to system resources. Operating systems that fail suddenly and with no incorporated failure state planning may leave the system available but with a reduced security protection capability. Preserving operating system state information also facilitates system restart and return to the operational mode of the organization with less disruption to mission-essential processes.

Abort refers to stopping a program or function before it has finished naturally. The term abort refers to both requested and unexpected terminations.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If only systems personnel are defined in SYS1.UADS and the DOWN Control Option values are set to DOWN(BW,SB,TN,OW), this is not a finding.

If non-systems personnel are defined in SYS1.UADS and the DOWN Control Option values are set to DOWN(BW,SB,TW,OW), this is not a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting as specified below and proceed with the change.

Setting if ONLY systems personnel are defined in SYS1.UADS: DOWN(BW,SB,TN,OW)

Setting if any non-systems personnel are defined in SYS1.UADS: DOWN(BW,SB,TW,OW)

CCI: CCI-001190

Group ID (Vulid): V-223957
Group Title: SRG-OS-000370-GPOS-00155
Rule ID: SV-223957r877798_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000840
Rule Title: The CA-TSS Facility Control Option must specify the sub option of MODE=FAIL.
Legacy ID: SV-107725
Legacy ID: V-98621

Vulnerability Discussion: Utilizing a whitelist provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities.

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

Verification of white-listed software occurs prior to execution or at system startup.

This requirement applies to operating system programs, functions, and services designed to manage system processes and configurations (e.g., group policies).

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY(FACILITY(ALL))

If the Facility Control Option does not specifies the sub option of "MODE=FAIL" for all facilities, this is a finding.

Fix Text: Evaluate the impact associated with implementation of the Facility Control Option MODE sub-option. Develop a plan of action to implement the Facility Control Option MODE sub-option setting to "MODE=FAIL" and proceed with the change.

CCI: CCI-001774

Group ID (Vulid): V-223958
Group Title: SRG-OS-000380-GPOS-00165

Rule ID: SV-223958r877799_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000850
Rule Title: CA-TSS ACID creation must use the EXP option.
Legacy ID: SV-107727
Legacy ID: V-98623

Vulnerability Discussion: Without providing this capability, an account may be created without a password. Non-repudiation cannot be guaranteed once an account is created if a user is not forced to change the temporary password upon initial logon.

Temporary passwords are typically used to allow access when new accounts are created or passwords are changed. It is common practice for administrators to create temporary passwords for user accounts which allow the users to log on, yet force them to change the password once they have successfully authenticated.

Check Content:
Ask the system administrator for the procedures for creating new ACIDs.

If the procedure contains the "EXP" option, this is not a finding.

Fix Text: Assure procedures to create New Acids include the "EXP" option.

Example:
TSS CREATE(USER02) NAME('ANDY POE')
TYPE(USER)
DEPARTMENT(PAYDEPT)
PASSWORD(INITIAL,60,EXP)
FACILITY(TSO)

CCI: CCI-002041

Group ID (Vulid): V-223959
Group Title: SRG-OS-000326-GPOS-00126
Rule ID: SV-223959r877800_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000860
Rule Title: The CA-TSS SUBACID Control Option must be set to U,8.
Legacy ID: SV-107729
Legacy ID: V-98625

Vulnerability Discussion: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned by the organizations.

Some programs and processes are required to operate at a higher privilege level and therefore should be excluded from the organization-defined software list after review.

Check Content:
From this ISPF Command Shell enter:
TSS MODIFY STATUS

If the SUBACID Control Option values are NOT set to "SUBACID(U,8)", this is a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting to "SUBACID(U,8)", and proceed with the change.

CCI: CCI-002233

Group ID (Vulid): V-223960
Group Title: SRG-OS-000326-GPOS-00126
Rule ID: SV-223960r877801_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000870
Rule Title: CA-TSS must use propagation control to eliminate ACID inheritance.
Legacy ID: SV-107731
Legacy ID: V-98627

Vulnerability Discussion: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned by the organizations.

Some programs and processes are required to operate at a higher privilege level and therefore should be excluded from the organization-defined software list after review.

Check Content:
From the ISPF Command Shell enter:

TSS MODIFY FACILITY(ALL)

enter
TSS MODIFY FACILITY(<FACILITY>)

If no Facility is defined with both the "MULTIUSER" and "ASUBM" attributes further analysis is not needed.

For each Facility with "MULTIUSER" and "ASUBM" attribute, review the @ACIDS report to determine which ACID(s) has (have) the following:

-A Master Facility of the Facility with "MULTIUSER" and "ASUBM" attribute, and,
-The Facility of "BATCH"

If each ACID that has the Master Facility of the Facility with "MULTIUSER" and "ASUBM" attribute and the Facility of "BATCH" is defined to the "PROPCNTL" resource class, this is not a finding.

Fix Text: Ensure an associated ACID exists for all batch jobs and propagation control is being used. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required.

The following Example shows the CONTROL-M STC ACID being owned to the PROPCNTL resource class:
TSS ADD(deptacid) PROPCNTL(control-m-acid)

CCI: CCI-002233

Group ID (Vulid): V-223961
Group Title: SRG-OS-000326-GPOS-00126
Rule ID: SV-223961r877802_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000880
Rule Title: IBM z/OS scheduled production batch ACIDs must specify the CA-TSS BATCH Facility, and the Batch Job Scheduler must be authorized to the Scheduled production CA-TSS batch ACID.
Legacy ID: V-98629
Legacy ID: SV-107733

Vulnerability Discussion: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned

by the organizations.

Some programs and processes are required to operate at a higher privilege level and therefore should be excluded from the organization-defined software list after review.

Check Content:
Refer to the documentation of the processes used for submission of batch jobs via an automated process (i.e., scheduler or other sources) and each of the associated userids.

Ensure that each identified batch ACID is sourced to a specific submission process used only for batch processing.

If the following guidance is true, this is not a finding.

-The job scheduler is cross-authorized to the batch ACIDs.
-The Facility of BATCH is specified for each batch ACID.
-Batch ACIDs with facilities other than BATCH should be questioned to ensure they are truly used for batch processing only, especially if a non-expiring password is used.
-The batch ACIDS may have the NOSUSPEND attribute.

Fix Text: Ensure associated ACIDs exist for all batch jobs and documentation justifying access to system resources is maintained and filed with the ISSO. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the required changes.

CCI: CCI-002233

Group ID (Vulid): V-223962
Group Title: SRG-OS-000327-GPOS-00127
Rule ID: SV-223962r877803_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000890
Rule Title: CA-TSS ADMINBY Control Option must be set to ADMINBY.
Legacy ID: V-98631
Legacy ID: SV-107735

Vulnerability Discussion: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Check Content:
From ISPF Command Shell enter:
TSS MODIFY STATUS

If the ADMINBY Control Option value is not set or set to "NOADMBY", this is a finding.

Fix Text: Ensure ADMINBY control option is set to "ADMINBY" to record who when and where information in the ACID security record for administrative changes.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting "ADMINBY" and proceed with the change.

CCI: CCI-002234

Group ID (Vulid): V-223963
Group Title: SRG-OS-000327-GPOS-00127
Rule ID: SV-223963r877804_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000900
Rule Title: CA-TSS LOG Control Option must be set to (SMF,INIT, SEC9, MSG).
Legacy ID: V-98633
Legacy ID: SV-107737

Vulnerability Discussion: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the LOG Control Option is NOT set to (SMF,INIT, SEC9, MSG), this is a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting as specified below and proceed with the change.

LOG(SMF,INIT, SEC9, MSG)

CCI: CCI-002234

Group ID (Vulid): V-223964
Group Title: SRG-OS-000327-GPOS-00127
Rule ID: SV-223964r877805_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000910
Rule Title: CA-TSS MSCA ACID password changes must be documented in the change log.
Legacy ID: V-98635
Legacy ID: SV-107739

Vulnerability Discussion: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Check Content:
From ISPF Command Shell enter:
Exec the CA-TSS TSSAUDIT Utility using CHANGES Control Statement.
Note: If running Quest NC-Pass, validate that the MSCA ACID has the FACILITY of NCPASS and SECURID resource in the ABSTRACT resource class.

If the MSCA password changes are documented in the change log, this is not a finding.

Fix Text: Ensure that the MSCA password changes are documented with comments in the TSS Recovery file. The TSS Recovery file will be of sufficient size to ensure that the change is documented.

CCI: CCI-002234

Group ID (Vulid): V-223965
Group Title: SRG-OS-000324-GPOS-00125
Rule ID: SV-223965r877806_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000920
Rule Title: The IBM z/OS IEASYMUP resource must be protected in accordance with proper security requirements.
Legacy ID: V-98637
Legacy ID: SV-107741

Vulnerability Discussion: Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

Check Content:
From the ISPF Command Shell enter:
TSS WHOOWNS IBMFAC(IEASYMUP)

If the TSS resources are owned or DEFPROT is specified for the resource class, this is not a finding.

Enter
TSS WHOHAS IBMFAC(IEASYMUP)

If TSS resource access authorizations restrict UPDATE and/or greater access to DASD administrators, Tape Library personnel, and system programming personnel, this is not a finding.

Fix Text: Ensure that the System level symbolic resources are defined to the FACILITY resource class and protected. UPDATE access to the System level symbolic resources are limited to System Programmers, DASD Administrators, and/or Tape Library personnel. All access is logged. Ensure the guidelines for the resources and/or generic equivalent are followed.

Limit access to the IEASYMUP resources to above personnel with UPDATE and/or greater access.

The following commands are provided as a sample for implementing resource controls:

TSS ADD(ADMIN) IBMFAC(IEASYMUP)

TSS PERMIT(<dasdsmpl>) IBMFAC(IEASYMUP) ACC(U) ACTION(AUDIT)
TSS PERMIT(<syspsmpl>) IBMFAC(IEASYMUP) ACC(U) ACTION(AUDIT)
TSS PERMIT(<tapesmpl>) IBMFAC(IEASYMUP) ACC(U) ACTION(AUDIT)

CCI: CCI-002235

Group ID (Vulid): V-223966
Group Title: SRG-OS-000324-GPOS-00125
Rule ID: SV-223966r877807_rule
Severity: CAT II

Rule Version (STIG-ID): TSS0-ES-000930
Rule Title: CA-TSS Default ACID must be properly defined.
Legacy ID: V-98639
Legacy ID: SV-107743

Vulnerability Discussion: Preventing non-privileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Check Content:
From the ISPF Command Shell enter:
TSS LIST STC

If *DEF* has action of *FAIL* this is not a finding.

If the default ACID is defined enter:
TSS List(<defined ACID>)

If the ACID has no access to resources and no facility access and sourced to the internal reader, this is not a finding.

If any of the above is untrue, this is a finding.

Fix Text: Ensure the default STC ACID is defined in accordance with the following restrictions. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as specified.

All STCs not defined to TSS will fail upon initiation. The following command may be used to associate all undefined STCs with a default action of FAIL:

TSS ADD(STC) PROCNAME(DEFAULT) ACID(FAIL)

If a valid requirement exists to establish a default STC, the following restrictions also apply:

a. The ISSO will maintain the written request, justification, and authorization.

b. The STC's ACID will have no other facilities permitted to it.

c. The STC's ACID will have a permission of DSN(*****) ACCESS(NONE).

TSS PERMIT(stc-acid) DSN(*****) ACCESS(NONE)

d. The STC's ACID will not have any permission to the resources available to TSS.

e. The STC's ACID will be sourced to the internal reader:

ADD(stc-acid) SOURCE(INTRDR)

f. An entry will be made in the STC table identifying the default ACID name as follows ("stc-acid" site defined):

TSS ADD(STC) PROCNAME(DEFAULT) ACID(stc-acid)

CCI: CCI-002235

Group ID (Vulid): V-223967
Group Title: SRG-OS-000324-GPOS-00125
Rule ID: SV-223967r877808_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000940
Rule Title: The CA-TSS BYPASS attribute must be limited to trusted STCs only.
Legacy ID: SV-107745
Legacy ID: V-98641

Vulnerability Discussion: Preventing non-privileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

Check Content:
From the ISPF Command Shell enter:
TSS LIST(STC)

If only STCs listed as trusted in the IBM z/OS MVS Initialization and Tuning Reference are granted the BYPASS privilege, this is not a finding.

Guidelines for reference:

Assign the TRUSTED attribute when one of the following conditions applies:
-The started procedure or address space creates or accesses a wide variety of unpredictably named data sets within your installation.

-Insufficient authority to an accessed resource might risk an unsuccessful IPL or other system problem.
-Avoid assigning TRUSTED to a z/OS started procedure or address space unless it is listed here or you are instructed to do so by the product documentation.

Additionally external security managers are candidates for trusted attribute. Any other started tasks not listed or not covered by the guidelines are a finding unless approval by the Authorizing Official AO.

Fix Text: Review the STC record for ACIDs with the BYPASS attribute. Ensure only those trusted STCs that are listed in the IBM z/OS MVS Initialization and Tuning Reference, have been granted this authority. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes.

Trusted STCs:

While the actual list may vary based on local site requirements and software configuration, the started tasks listed in the IBM z/OS MVS Initialization and Tuning Reference is an approved list of started tasks that may be considered trusted started procedures.

Guidelines for reference:

Assign the TRUSTED attribute when one of the following conditions applies:
-The started procedure or address space creates or accesses a wide variety of unpredictably named data sets within your installation.
-Insufficient authority to an accessed resource might risk an unsuccessful IPL or other system problem.
-Avoid assigning TRUSTED to a z/OS started procedure or address space unless it is listed here or you are instructed to do so by the product documentation.

Additionally external security managers are candidates for trusted attribute. Any other started tasks not; listed or not covered by the guidelines are a finding unless approval by the Authorizing Official AO.

CCI: CCI-002235

Group ID (Vulid): V-223968
Group Title: SRG-OS-000324-GPOS-00125
Rule ID: SV-223968r877809_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000950
Rule Title: CA-TSS MSCA ACID must perform security administration only.
Legacy ID: SV-107747
Legacy ID: V-98643

Vulnerability Discussion: Preventing non-privileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

Check Content:
From the ISPF Command Shell enter:
TSS LIST(ACIDS) DATA(ALL,PA) TYPE(SCA)

If the MSCA ACID has access limited to performing security administration functions only, this is not a finding.

Below is an example of allowed setup for MSCA account and authorities. "MSCA" as the Accessorid is merely an example here, which is site determined. List is not all inclusive. The primary SCA for the domain will be listed within the "NAME" field since they are responsible for the MSCA ACID.

ACCESSORID = MSCA NAME = "primary SCA"
TYPE = MASTER
FACILITY = BATCH
PROFILES = SECURID
ATTRIBUTES = AUDIT,CONSOLE,NOATS
data set = %. *.
data set = ***** +.
VOLUMES = *(G)
XA data set = SYS3.TSS.BACKUP
ACCESS = UPDATE
ACTION = AUDIT
---------- ADMINISTRATION AUTHORITIES
RESOURCE = *ALL*
ACCESS = ALL
ACID = *ALL*
FACILITIES = *ALL*
LIST DATA = *ALL*,PROFILES,PASSWORD,SESSKEY
MISC1 = *ALL*
MISC2 = *ALL*
MISC4 = *ALL*
MISC8 = *ALL*

MISC9 = *ALL*

NOTE 1: Update access to the backup security database is required by the MSCA account anytime the ISSO needs to run/submit the TSS Utility called TSSFAR. MSCA account may from time to time be required to have additional access for the period of project such as Extending the Security Database.

NOTE 2: MSCA account must be used for such items as: TSSFAR, EXTENDING Security Database, creating SCA/LSCA accounts, working with LSCA accounts (scoping, admin rights, etc.). Most often the ISSO staff will utilize their normal SCA account. The MSCA account will not be anyone's primary security administrative account.

Fix Text: The ISSO will review the MSCA and ensure access granted is limited to those resources necessary to support the security administration function. Evaluate the impact of correcting the deficiency and develop a plan of action to implement the changes.

Below is an example of allowed setup for MSCA account and authorities. "MSCA" as the Accessorid is merely an example here, which is site determined. List is not all inclusive. The primary SCA for the domain will be listed within the "NAME" field since they are responsible for the MSCA ACID.

ACCESSORID = MSCA NAME = "primary SCA"
TYPE = MASTER
FACILITY = BATCH
PROFILES = SECURID
ATTRIBUTES = AUDIT,CONSOLE,NOATS
data set = %. *.
data set = ***** +.
VOLUMES = *(G)
XA data set = SYS3.TSS.BACKUP
ACCESS = UPDATE
ACTION = AUDIT
---------- ADMINISTRATION AUTHORITIES
RESOURCE = *ALL*
ACCESS = ALL
ACID = *ALL*
FACILITIES = *ALL*
LIST DATA = *ALL*,PROFILES,PASSWORD,SESSKEY
MISC1 = *ALL*
MISC2 = *ALL*
MISC4 = *ALL*
MISC8 = *ALL*
MISC9 = *ALL*

NOTE 1: Update access to the backup security database is required by the MSCA account anytime the ISSO needs to run/submit the TSS Utility called TSSFAR. MSCA account may from

time to time be required to have additional access for the period of project such as Extending the Security Database.

NOTE 2: MSCA account must be used for such items as: TSSFAR, EXTENDING Security Database, creating SCA/LSCA accounts, working with LSCA accounts (scoping, admin rights, etc). Most often the ISSO staff will utilize their normal SCA account. The MSCA account will not be anyone's primary security administrative account.

NOTE 3: MSCA account must be limited in access, to least privileged access of resources required to function.

NOTE 4: If running Quest NC-Pass, validate in ZNCP0020 that the MSCA ACID has the FACILITY of NCPASS and SECURID resource in the ABSTRACT resource class.

CCI: CCI-002235

Group ID (Vulid): V-223969
Group Title: SRG-OS-000324-GPOS-00125
Rule ID: SV-223969r877810_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-ES-000960
Rule Title: CA-TSS ACIDs granted the CONSOLE attribute must be justified.
Legacy ID: SV-107749
Legacy ID: V-98645

Vulnerability Discussion: Preventing non-privileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

Check Content:
Execute TSS Report TSS AUDIT with PRIVILEGES control statement PRIVILEGES [SHORT]. For more information TSSAUDIT reports refer to the CA-TSS Report and Tracking Guide. Refer to the resulting report.

If ACIDs with CONSOLE authority are limited to authorized SCA security administrators and the system programmers that maintain the CA-TSS software product only, this is not a finding.

Fix Text: Review all ACIDs with the CONSOLE attribute. Ensure access is limited to authorized SCA security administrators only. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes. Ensure documentation providing justification for access is maintained and filed with the ISSO.

CCI: CCI-002235

Group ID (Vulid): V-223970
Group Title: SRG-OS-000324-GPOS-00125
Rule ID: SV-223970r877811_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000970
Rule Title: CA-TSS ACIDs defined as security administrators must have the NOATS attribute.
Legacy ID: SV-107751
Legacy ID: V-98647

Vulnerability Discussion: Preventing non-privileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

Check Content:
Execute TSS Report TSS AUDIT with PRIVILEGES control statement PRIVILEGES [SHORT]. For more information TSSAUDIT reports refer to the CA-TSS Report and Tracking Guide. Refer to the resulting report.

If all security administrators have the "NOATS" attribute, this is not a finding.

Fix Text: Review all security administrator ACIDs. Ensure the "NOATS" attribute has been assigned. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes.

NOTE: The NOATS attribute may be added to an ACID or an ACID's PROFILE.

The following command may be issued to determine if the NOATS attribute is defined to an ACID or an ACID's PROFILE:

tss list(<acid>) data(basic,profile)

CCI: CCI-002235

Group ID (Vulid): V-223971
Group Title: SRG-OS-000329-GPOS-00128
Rule ID: SV-223971r877812_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000980
Rule Title: The CA-TSS PTHRESH Control Option must be properly set.
Legacy ID: V-98649
Legacy ID: SV-107753

Vulnerability Discussion: By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS

If the PTHRESH Control Option value is not set to "PTHRESH(2)", this is a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting as specified following and proceed with the change.

PTHRESH(2)

CCI: CCI-002238

Group ID (Vulid): V-223972
Group Title: SRG-OS-000279-GPOS-00109
Rule ID: SV-223972r877813_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-ES-000990
Rule Title: CA-TSS VTHRESH Control Option values specified must be set to (10,NOT,CAN).
Legacy ID: V-98651
Legacy ID: SV-107755

Vulnerability Discussion: Automatic session termination addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions.

Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated.

Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on information system use.

This capability is typically reserved for specific operating system functionality where the system owner, data owner, or organization requires additional assurance.

Check Content:
From the ISPF Control Shell enter:
TSS MODIFY STATUS

If the VTHRESH Control Option values are not set to "VTHRRESH(10,NOT,CAN)", this is a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option setting to "VTHRESH(10,NOT,CAN)", and proceed with the change.

CCI: CCI-002361

Group ID (Vulid): V-223973
Group Title: SRG-OS-000023-GPOS-00006
Rule ID: SV-223973r877814_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-FT-000010
Rule Title: IBM z/OS FTP.DATA configuration statements must have a proper banner statement with the Standard Mandatory DoD Notice and Consent Banner.
Legacy ID: SV-107757
Legacy ID: V-98653

Vulnerability Discussion: Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007

Check Content:
Refer to the FTP.DATA file specified on the SYSFTPD DD statement in the FTP started task JCL. The SYSFTPD DD statement is optional. The search order for FTP.DATA is:
/etc/ftp.data
SYSFTPD DD statement
jobname.FTP.DATA
SYS1.TCPPARMS(FTPDATA)
tcpip.FTP.DATA

Examine the BANNER statement.

If the BANNER statement in the FTP Data configuration file specifies an HFS file or data set that contains a logon banner, this is not a finding.

The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Fix Text: Ensure the BANNER statement in the FTP Data configuration file specifies an HFS file or z/OS data set that contains a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

CCI: CCI-000048

CCI: CCI-000050

Group ID (Vulid): V-223974
Group Title: SRG-OS-000032-GPOS-00013
Rule ID: SV-223974r877815_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-FT-000020

Rule Title: IBM z/OS SMF recording options for the FTP server must be configured to write SMF records for all eligible events.
Legacy ID: V-98655
Legacy ID: SV-107759

Vulnerability Discussion: Remote access services, such as those providing remote access to network devices and information systems, which lack automated monitoring capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Automated monitoring of remote access sessions allows organizations to detect cyberattacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote access capabilities, such as Remote Desktop Protocol (RDP), on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Satisfies: SRG-OS-000032-GPOS-00013, SRG-OS-000392-GPOS-00172

Check Content:
If FTPDATA is configured with the following SMF statements, this is not a finding.

FTP.DATA Configuration Statements
SMF TYPE119
SMFJES TYPE119
SMFSQL TYPE119
SMFAPPE [Not coded or commented out]
SMFDEL [Not coded or commented out]
SMFEXIT [Not coded or commented out]
SMFLOGN [Not coded or commented out]
SMFREN [Not coded or commented out]
SMFRETR [Not coded or commented out]
SMFSTOR [Not coded or commented out]

Fix Text: Configure SMF options to conform to the specifications in the FTPDATA Configuration Statements below or that they are commented out.

SMF TYPE119
SMFJES TYPE119
SMFSQL TYPE119
SMFAPPE [Not coded or commented out]
SMFDEL [Not coded or commented out]
SMFEXIT [Not coded or commented out]

SMFLOGN [Not coded or commented out]
SMFREN [Not coded or commented out]
SMFRETR [Not coded or commented out]
SMFSTOR [Not coded or commented out]

The FTP Server can provide audit data in the form of SMF records. SMF record type 119, the TCP/IP Statistics record, can be written with the following subtypes:

70 - Append
70 - Delete and Multiple Delete
72 - Invalid Logon Attempt
70 - Rename
70 - Get (Retrieve) and Multiple Get
70 - Put (Store and Store Unique) and Multiple Put

SMF data produced by the FTP Server provides transaction information for both successful and unsuccessful FTP commands. This data may provide valuable information for security audit activities. Type 119 records use a more standard format and provide more information.

CCI: CCI-000067

CCI: CCI-002884

Group ID (Vulid): V-223975
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223975r877816_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-FT-000030
Rule Title: CA-TSS permission bits and user audit bits for HFS objects that are part of the FTP server component must be properly configured.
Legacy ID: SV-107761
Legacy ID: V-98657

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
From the ISPF Command Shell enter:
omvs

At the input line enter:
cd /usr/sbin/
enter
ls -alW

If the following File permission and user Audit Bits are true, this is not a finding.
/usr/sbin/ftpd 1740 fff
/usr/sbin/ftpdns 1755 fff
/usr/sbin/tftpd 0644 faf
cd
ls -alW

If the following file permission and user Audit Bits are true, this is not a finding.
/etc/ftp.data 0744 faf
/etc/ftp.banner 0744 faf

NOTES: Some of the files listed above are not used in every configuration. The absence of a file is not considered a finding.

The /usr/sbin/ftpd and /usr/sbin/ftpdns objects are symbolic links to /usr/lpp/tcpip/sbin/ftpd and /usr/lpp/tcpip/sbin/ftpdns respectively. The permission and user audit bits on the targets of the symbolic links must have the required settings.

The /etc/ftp.data file may not be the configuration file the server uses. It is necessary to check the SYSFTPD DD statement in the FTP started task JCL to determine the actual file.

The TFTP Server does not perform any user identification or authentication, allowing any client to connect to the TFTP Server. Due to this lack of security, the TFTP Server will not be used. The TFTP Client is not secured from use. The permission bits for /usr/sbin/tftpd should be set to 644.

The /etc/ftp.banner file may not be the banner file the server uses. It is necessary to check the BANNER statement in the FTP Data configuration file to determine the actual file. Also, the permission bit setting for this file must be set as indicated in the table above. A more restrictive

set of permissions is not permitted.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
- no auditing

Fix Text: With the assistance of a systems programmer with UID(0) and/or SUPERUSER access, configure the UNIX permission bits and user audit bits on the HFS directories and files for the FTP Server to conform to the specifications in the table below:

FTP Server HFS Object Security Settings
File Permission Bits User Audit Bits
/usr/sbin/ftpd 1740 fff
/usr/sbin/ftpdns 1755 fff
/usr/sbin/tftpd 0644 faf
/etc/ftp.data 0744 faf
/etc/ftp.banner 0744 faf

The /usr/sbin/ftpd and /usr/sbin/ftpdns objects are symbolic links to /usr/lpp/tcpip/sbin/ftpd and /usr/lpp/tcpip/sbin/ftpdns respectively. The permission and user audit bits on the targets of the symbolic links must have the required settings.

The TFTP Server does not perform any user identification or authentication, allowing any client to connect to the TFTP Server. Due to this lack of security, the TFTP Server will not be used. The TFTP Client is not secured from use.

The /etc/ftp.data file may not be the configuration file the server uses. It is necessary to check the SYSFTPD DD statement in the FTP started task JCL to determine the actual file.

The /etc/ftp.banner file may not be the banner file the server uses. It is necessary to check the BANNER statement in the FTP Data configuration file to determine the actual file.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
- no auditing

Some of the files listed above (e.g., /etc/ftp.data) are not used in every configuration. While the absence of a file is generally not a security issue, the existence of a file that has not been properly secured can often be an issue. Therefore, all files that do exist should have the specified permission and audit bit settings.

The following commands can be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

chmod 1740 /usr/lpp/tcpip/sbin/ftpd
chaudit rwx=f /usr/lpp/tcpip/sbin/ftpd
chmod 1755 /usr/lpp/tcpip/sbin/ftpdns
chaudit rwx=f /usr/lpp/tcpip/sbin/ftpdns
chmod 0744 /etc/ftp.data
chaudit w=sf,rx+f /etc/ftp.data
chmod 0744 /etc/ftp.banner
chaudit w=sf,rx+f /etc/ftp.banner

CCI: CCI-000213

Group ID (Vulid): V-223976
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223976r877817_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-FT-000040
Rule Title: IBM z/OS data sets for the FTP server must be properly protected.
Legacy ID: SV-107763
Legacy ID: V-98659

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
If WRITE and ALLOCATE access to the data set containing the FTP Data configuration file is restricted to systems programming personnel this is not a finding.

Note: READ access to all authenticated users is permitted.

If WRITE and ALLOCATE access to the data set containing the FTP Data configuration file is logged this is not a finding.

If WRITE and ALLOCATE access to the data set containing the FTP banner file is restricted to systems programming personnel this is not a finding.

Note: READ access to the data set containing the FTP banner file is permitted to all authenticated users.

Notes: The MVS data sets mentioned above are not used in every configuration. Absence of a data set will not be considered a finding.
The data set containing the FTP Data configuration file is determined by checking the SYSFTPD DD statement in the FTP started task JCL.
The data set containing the FTP banner file is determined by checking the BANNER statement in the FTP Data configuration file.

Fix Text: Review the data set access authorizations defined to the ACP for the FTP.DATA and FTP.BANNER files. Configure these data sets to be protected as follows:

CCI: CCI-000213

Group ID (Vulid): V-223977
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223977r877818_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-FT-000050
Rule Title: IBM z/OS FTP Control cards must be properly stored in a secure PDS file.
Legacy ID: SV-107765
Legacy ID: V-98661

Vulnerability Discussion: Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Check Content:
Ask the System administrator fora list(s) of the locations for all FTP Control cards within a given application/AIS, ensuring no FTP control cards are within in-stream JCL, JCL libraries or any open access data sets.

If access to PDS files where FTP Control cards are stored are not restricted to appropriate personnel this is a finding.

Fix Text: Make sure that the FTP control Cards for each FTP are stored in a secure PDS and that they are not placed in the JCL libraries or in the in-stream JCL for each FTP.

CCI: CCI-000202

CCI: CCI-000366

Group ID (Vulid): V-223978
Group Title: SRG-OS-000096-GPOS-00050
Rule ID: SV-223978r877819_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-FT-000060
Rule Title: IBM z/OS user exits for the FTP server must not be used without proper approval and documentation.

Legacy ID: V-98663
Legacy ID: SV-107767

Vulnerability Discussion: In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., VPN and IPS); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the operating system must support the organizational requirements, providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

Check Content:
Refer to the Data configuration file specified on the SYSFTPD DD statement in the FTP started task JCL.

Refer to the file(s) allocated by the STEPLIB DD statement in the FTP started task JCL.

Refer to the libraries specified in the system Linklist and LPA.

If any FTP Server exits are in use, identify them and validate that they were reviewed for integrity and approved by the site AO.

Refer to the following items are in effect for FTP Server user exits:

The FTCHKCMD, FTCHKIP, FTCHKJES, FTCHKPWD, FTPSMFEX and FTPOSTPR modules are not located in the FTP daemon's STEPLIB, Linklist, or LPA.

NOTE: The ISPF ISRFIND utility can be used to search the system Linklist and LPA for specific modules.

If both of the above are true, this is not a finding.

If any FTP Server user exits are implemented and the site has not had the site systems programmer verify the exit was securely written and installed, this is a finding.

Fix Text: Review the configuration statements in the FTP.DATA file. Review the FTP daemon

STEPLIB, system Linklist, and Link Pack Area libraries. If FTP Server exits are enabled or present, and have not been approved by the site ISSM and not securely written and implemented by the site systems programmer, they should not be installed. Verify that none of the following exits are installed unless they have met the requirements listed above:
FTCHKCMD
FTCHKIP
FTCHKJES
FTCHKPWD
FTPOSTPR
FTPSMFEX

CCI: CCI-000382

Group ID (Vulid): V-223979
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223979r877820_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-FT-000070
Rule Title: The IBM z/OS FTP server daemon must be defined with proper security parameters.
Legacy ID: SV-107769
Legacy ID: V-98665

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
From the ISPD Command Shell enter:
TSS LIST(FTPD) SEGMENT(OMVS)

NOTE: The JCL member is typically named FTPD

If the FTPD ACID has the STC facility, this is not a finding.

If the FTPD ACID has the following z/OS UNIX attributes, this is not a finding.

UID(0), HOME directory '/', shell program /bin/sh.

Fix Text: Configure FTP daemon with the following items:

-The FTP daemon is started from a JCL procedure library defined to JES2.

NOTE: The JCL member is typically named FTPD.

-The FTP daemon ACID is FTPD.

-The FTPD ACID has the STC facility.

-The FTPD ACID has the following z/OS UNIX attributes:
UID(0), HOME directory '/', shell program /bin/sh.

For example:
TSS CREATE(FTPD) TYPE(USER) NAME(FTPD)
DEPT(existing-dept) FACILITY(STC) PASSWORD(password,0)
TSS ADD(FTPD) DFLTGRP(STCTCPX) GROUP(STCTCPX)
TSS ADD(FTPD) SOURCE(INTRDR)
TSS ADD(FTPD) UID(0) HOME(/) OMVSPGM(/bin/sh)
TSS ADD(FTPD) MASTFAC(TCP)
TSS ADD(STC) PROCNAME(FTPD) ACID(FTPD)
TSS PERMIT(FTPD) IBMFAC(BPX.DAEMON) ACCESS(READ)
TSS PERMIT(FTPD) IBMFAC(BPX.POE) ACCESS(READ)
TSS PERMIT(FTPD) SERVAUTH(EZB.STACKACCESS.)ACCESS(READ)

CCI: CCI-000764

Group ID (Vulid): V-223980
Group Title: SRG-OS-000163-GPOS-00072
Rule ID: SV-223980r877821_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-FT-000080
Rule Title: IBM z/OS FTP.DATA configuration for the FTP server must have the INACTIVE statement properly set.
Legacy ID: SV-107771
Legacy ID: V-98667

Vulnerability Discussion: Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Check Content:
Refer to the file specified on the SYSFTPD DD statement in the FTP started task JCL.

If the INACTIVE statement is coded with a value greater than "600", this is a finding.

If the INACTIVE statement is coded with a value of "0", this is a finding.

If there is no INACTIVE statement coded or the INACTIVE statement is commented out, this is a finding.

Fix Text: Code the FTPD configuration file to include the INACTIVE statement with a value between "1" and "600".

CCI: CCI-001133

Group ID (Vulid): V-223981
Group Title: SRG-OS-000163-GPOS-00072
Rule ID: SV-223981r877822_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-FT-000090
Rule Title: IBM z/OS startup parameters for the FTP server must have the INACTIVE statement properly set.
Legacy ID: SV-107773
Legacy ID: V-98669

Vulnerability Discussion: Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, and de-allocating networking assignments at the application level if multiple application sessions are

using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Check Content:
Refer to the Profile configuration file specified on the PROFILE DD statement in the TCPIP started task JCL.

If all the items below are true, this is not a finding.

If any of the items below are untrue, this is a finding.

The following items are in effect for the FTP daemon's started task JCL:

-The SYSTCPD and SYSFTPD DD statements specify the TCP/IP Data and FTP Data configuration files respectively.
-The ANONYMOUS keyword is not coded on the PARM parameter on the EXEC statement.
-The ANONYMOUS=logonid combination is not coded on the PARM parameter on the EXEC statement.
-The INACTIVE keyword is not coded on the PARM parameter on the EXEC statement.

The AUTOLOG statement block can be configured to have TCP/IP start the FTP Server. The FTP entry (e.g., FTPD) can include the PARMSTRING parameter to pass parameters to the FTP procedure when started.

NOTE: Parameters passed on the PARMSTRING parameter override parameters specified in the FTP procedure.

If an FTP entry is configured in the AUTOLOG statement block in the TCP/IP Profile configuration file, ensure the following items are in effect:

-The ANONYMOUS keyword is not coded on the PARMSTRING parameter.
-The ANONYMOUS=logonid combination is not coded on the PARMSTRING parameter.
-The INACTIVE keyword is not coded on PARMSTRING parameter.

Fix Text: Review the FTP daemon's started task JCL. Ensure that the ANONYMOUS and INACTIVE startup parameters are not specified and configuration file names are specified on the appropriate DD statements.

The FTP daemon program can accept parameters in the JCL procedure that is used to start the daemon. The ANONYMOUS and ANONYMOUS= keywords are designed to allow anonymous FTP connections. The INACTIVE keyword is designed to set the timeout value for inactive connections. Control of these options is recommended through the configuration file statements rather than the startup parameters.

The systems programmer responsible for supporting ICS will ensure that the startup parameters for the FTP daemon does not include the ANONYMOUS, ANONYMOUS=, or INACTIVE keywords.

During initialization the FTP daemon searches multiple locations for the TCPIP.DATA and FTP.DATA files according to fixed sequences. In the daemon's started task JCL, Data Definition (DD) statements will be used to specify the locations of the files. The SYSTCPD DD statement identifies the TCPIP.DATA file and the SYSFTPD DD statement identifies the FTP.DATA file.

The systems programmer responsible for supporting ICS will ensure that the FTP daemon's started task JCL specifies the SYSTCPD and SYSFTPD DD statements for configuration files.

CCI: CCI-001133

Group ID (Vulid): V-223982
Group Title: SRG-OS-000228-GPOS-00088
Rule ID: SV-223982r877823_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-FT-000100
Rule Title: IBM z/OS FTP.DATA configuration statements for the FTP server must specify the Standard Mandatory DoD Notice and Consent Banner statement.
Legacy ID: V-98671
Legacy ID: SV-107775

Vulnerability Discussion: Display of a standardized and approved use notification before granting access to the publicly accessible operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense,

personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read & consent to terms in IS user agreem't."

Check Content:
Refer to the file specified on the SYSFTPD DD statement in the FTP started task JCL.

If the BANNER statement is not coded or is commented out, this is a finding.

Fix Text: Code the FTPD configuration file to include the BANNER statement that points to the Standard Mandatory DoD Notice and Consent Banner statement.

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

Group ID (Vulid): V-223983
Group Title: SRG-OS-000228-GPOS-00088
Rule ID: SV-223983r877824_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-FT-000110
Rule Title: The IBM z/OS warning banner for the FTP server must be properly specified.
Legacy ID: V-98673
Legacy ID: SV-107777

Vulnerability Discussion: Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See

User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read & consent to terms in IS user agreem't."

Check Content:
Refer to the FTP.DATA file specified on the SYSFTPD DD statement in the FTP started task JCL. The SYSFTPD DD statement is optional. The search order for FTP.DATA is:
/etc/ftp.data
SYSFTPD DD statement
jobname.FTP.DATA
SYS1.TCPPARMS(FTPDATA)
tcpip.FTP.DATA

Examine the BANNER statement.

If the BANNER statement in the FTP Data configuration file specifies an HFS file or data set that contains a logon banner, this is not a finding.

The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Fix Text: Ensure the BANNER statement in the FTP Data configuration file specifies an HFS file or z/OS data set that contains a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

Group ID (Vulid): V-223984
Group Title: SRG-OS-000368-GPOS-00154
Rule ID: SV-223984r877825_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-FT-000120
Rule Title: The IBM z/OS TFTP server program must be properly protected.
Legacy ID: V-98675
Legacy ID: SV-107779

Vulnerability Discussion: Control of program execution is a mechanism used to prevent execution of unauthorized programs. Some operating systems may provide a capability that runs counter to the mission or provides users with functionality that exceeds mission requirements. This includes functions and services installed at the operating system level.

Some of the programs, installed by default, may be harmful or may not be necessary to support essential organizational operations (e.g., key missions, functions). Removal of executable programs is not always possible; therefore, establishing a method of preventing program execution is critical to maintaining a secure system baseline.

Methods for complying with this requirement include restricting execution of programs in certain environments, while preventing execution in other environments; or limiting execution of certain program functionality based on organization-defined criteria (e.g., privileges, subnets, sandboxed environments, or roles).

Check Content:
From the ISPF Command Shell enter:
TSS WHOOWNS PROGRAM(*)

If the Program resources TFTPD and EZATD are owned appropriately in the PROGRAM resource class, this is not a finding.

Enter
TSS WHOHAS(TFTPD)
TSS WHOHAS(EZATD)

If no access to the program resources TFTPD and EZATD is permitted, this is not a finding.

Fix Text: Evaluate the impact of implementing the following change. Develop a plan of action and implement the change as required. Ensure that the EZATD program and its alias TFTPD are

defined to CA-TSS and no access to the program resources TFTPD and EZATD is permitted. The following commands provide a sample of how to protect the TFTP server program by assigning ownership and no permissions: TSS ADD(ADMIN) PROGRAM(TFTPD,EZATD)

CCI: CCI-001764

Group ID (Vulid): V-255896
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-255896r877951_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-FT-000130
Rule Title: IBM z/OS FTP.DATA configuration statements for the FTP Server must be specified in accordance with requirements.
Legacy ID: V-98185
Legacy ID: SV-107289

Vulnerability Discussion: This requirement is intended to cover both traditional interactive logons to information systems and general accesses to information systems that occur in other types of architectural configurations (e.g., service-oriented architectures).

Check Content:
Refer to the Data configuration file specified on the SYSFTPD DD statement in the FTP started task JCL.

If the UMASK statement is coded with a value of "077", this is not a finding.

Fix Text: Configure the FTP configuration to include the UMASK statement with a value of "077".

If the FTP Server requires a UMASK value less restrictive than "077", requirements should be justified and documented with the ISSO.

CCI: CCI-000366

Group ID (Vulid): V-255940
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-255940r881312_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-IC-000010
Rule Title: IBM Integrated Crypto Service Facility (ICSF) Configuration parameters must be

correctly specified.
Legacy ID: V-18014
Legacy ID: SV-95665

Vulnerability Discussion: IBM Integrated Crypto Service Facility (ICSF) product has the ability to use privileged functions and/or have access to sensitive data. Failure to properly configure parameter values could potentially the integrity of the base product which could result in compromising the operating system or sensitive data.

Check Content:
Refer to the CSFPRMxx member in the logical PARMLIB concatenation.

If the configuration parameters are specified as follows this is not a finding.

REASONCODES(ICSF)
COMPAT(NO)
SSM(NO)
SSM can be dynamically set by defining the CSF.SSM.ENABLE SAF profile within the XFACILIT resource
Class. If this profile is not limited to authorized personnel this is a finding.
CHECKAUTH(YES)
FIPSMODE(YES,FAIL(YES))
AUDITKEYLIFECKDS (TOKEN(YES),LABEL(YES)).
AUDITKEYLIFEPKDS (TOKEN(YES),LABEL(YES)).
AUDITKEYLIFETKDS (TOKENOBJ(YES),SESSIONOBJ(YES)).
AUDITKEYUSGCKDS (TOKEN(YES),LABEL(YES),INTERVAL(n)).
AUDITKEYUSGPKDS (TOKEN(YES),LABEL(YES),INTERVAL(n)).
AUDITPKCS11USG (TOKENOBJ(YES),SESSIONOBJ(YES),NOKEY(YES),INTERVAL(n)).

DEFAULTWRAP -This parameter can be determined by the site. ENHANCED wrapping specifies the new X9.24 compliant CBC wrapping is used.
If DEFAULTWRAP is not specified, the default wrapping
method will be ORIGINAL for both internal and external tokens. Starting with ICSF FMID HCR77C0, the value for this option can be updated without restarting ICSF by using either the SETICSF command or the ICSF Multi-Purpose service. If this access is not restricted to appropriate personnel, this is a finding. (Note: Other options may be site defined.

Fix Text: Evaluate the impact associated with implementation of the control options. Develop a plan of action to implement the control options for CSFPRMxx as specified below:

REASONCODES(ICSF)
COMPAT(NO)

SSM(NO)
SSM can be dynamically set by defining the CSF.SSM.ENABLE SAF profile within the XFACILIT resource
Class. This profile must limited to authorized personnel.

CHECKAUTH(YES)
FIPSMODE(YES,FAIL(YES))
AUDITKEYLIFECKDS (TOKEN(YES),LABEL(YES)).
AUDITKEYLIFEPKDS (TOKEN(YES),LABEL(YES)).
AUDITKEYLIFETKDS (TOKENOBJ(YES),SESSIONOBJ(YES)).
AUDITKEYUSGCKDS (TOKEN(YES),LABEL(YES),INTERVAL(n)).
AUDITKEYUSGPKDS (TOKEN(YES),LABEL(YES),INTERVAL(n)).
AUDITPKCS11USG (TOKENOBJ(YES),SESSIONOBJ(YES),NOKEY(YES),INTERVAL(n)).

DEFAULTWRAP -This parameter can be determined by the site. ENHANCED wrapping specifies the new X9.24 compliant CBC wrapping is used.
If DEFAULTWRAP is not specified, the default wrapping
method will be ORIGINAL for both internal and external tokens. Starting with ICSF FMID HCR77C0, the value for this option can be updated without restarting ICSF by using either the SETICSF command or the ICSF Multi-Purpose service. This access must be restricted to appropriate personnel.
Note: Other options may be site defined.

CCI: CCI-000366

Group ID (Vulid): V-255941
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-255941r881315_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-IC-000020
Rule Title: IBM Integrated Crypto Service Facility (ICSF) install data sets are not properly protected.
Legacy ID: V-16932
Legacy ID: SV-30550

Vulnerability Discussion: IBM Integrated Crypto Service Facility (ICSF) product has the ability to use privileged functions and/or have access to sensitive data. Failure to properly restrict access to their data sets could result in violating the integrity of the base product which could result in compromising the operating system or sensitive data.

Check Content:
Verify that access to the IBM IntegrTated Crypto Service Facility (ICSF) install data sets are properly restricted.

Execute a data set list of access to the IBM Integrated Crypto Service Facility (ICSF) install data sets

If the TSS data set rules for the data sets does not restrict UPDATE and/or ALL access to systems programming personnel this is a finding.

If the TSS data set rules for the data sets does not specify that all (i.e., failures and successes) UPDATE and/or ALL access will be logged this is a finding.

Fix Text: Ensure that update and allocate access to IBM Integrated Crypto Service Facility (ICSF) install data sets is limited to System Programmers only, and all update and allocate access is logged. Read access can be given to Auditors and any other users that have a valid requirement to utilize these data sets.

The installing Systems Programmer will identify and document the product data sets and categorize them according to who will have update and alter access and if required that all update and allocate access is logged. He will identify if any additional groups have update access for specific data sets, and once documented he will work with the IAO to see that they are properly restricted to the ACP (Access Control Program) active on the system.

Data sets to be protected will be:
SYS1.CSF

The following commands are provided as a sample for implementing data set controls:

TSS PERMIT(syspaudt) DSN(SYS1.CSF.) ACCESS(R)
TSS PERMIT(tstcaudt) DSN(SYS1.CSF.) ACCESS(R)
TSS PERMIT(icsfusrs) DSN(SYS1.CSF.) ACCESS(R)
TSS PERMIT(syspaudt) DSN(SYS1.CSF.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(tstcaudt) DSN(SYS1.CSF.) ACCESS(ALL) ACTION(AUDIT)

CCI: CCI-000213

CCI: CCI-002264

Group ID (Vulid): V-255944
Group Title: SRG-OS-000259-GPOS-00100
Rule ID: SV-255944r881324_rule

Severity: CAT II
Rule Version (STIG-ID): TSS0-IC-000030
Rule Title: IBM Integrated Crypto Service Facility (ICSF) STC data sets must be properly protected.
Legacy ID: V-17067
Legacy ID: SV-30565

Vulnerability Discussion: IBM Integrated Crypto Service Facility (ICSF) STC data sets have the ability to use privileged functions and/or have access to sensitive data. Failure to properly restrict access to their data sets could result in violating the integrity of the base product which could result in compromising the operating system or sensitive data.

Check Content:
Verify that access to the IBM Integrated Crypto Service Facility (ICSF) STC data sets are properly restricted. The data sets to be protected are identified in the data set referenced in the CSFPARM DD statement of the ICSF started task(s) and/or batch job(s); the entries for CKDSN and PKDSN specify the data sets. If the following guidance is true, this is not a finding.

If the TSS data set access authorizations do not restrict READ access to auditors, this is a finding.

If the TSS data set access authorizations do not restrict WRITE and/or greater access to systems programming personnel, this is a finding.

If the TSS data set access authorizations do not restrict WRITE and/or greater access to the product STC(s) and/or batch job(s), this is a finding.

Fix Text: The ISSO will ensure that WRITE and/or greater access to IBM Integrated Crypto Service Facility (ICSF) STC and/or batch data sets are limited to system programmers and ICSF STC and/or batch jobs only. READ access can be given to auditors at the ISSO's discretion.

The installing systems programmer will identify and document the product data sets and categorize them according to who will have what type of access and if required which type of access is logged. The installing systems programmer will identify any additional groups requiring access to specific data sets, and once documented the installing systems programmer will work with the ISSO to see that they are properly restricted to the ACP (Access Control Program) active on the system.

(Note: The data sets and/or data set prefixes identified below are examples of a possible installation. The actual data sets and/or prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.)

The data sets to be protected are identified in the data set referenced in the CSFPARM DD statement of the ICSF started task(s) and/or batch job(s); the entries for CKDSN and PKDSN

specify the data sets.

Note: Currently on most CSD systems, the CKDSN specifies SYS3.CSF.CKDS and PKDSN specifies SYS3.CSF.PKDS.

The following commands are provided as a sample for implementing data set controls:

TSS PERMIT(audtaudt) DSN(SYS3.CDS.) ACCESS(R)
TSS PERMIT(syspaudt) DSN(SYS3.CDS.) ACCESS(R)
TSS PERMIT(tstcaudt) DSN(SYS3.CDS.) ACCESS(R)
TSS PERMIT(icsfstc) DSN(SYS3.CDS.) ACCESS(R)
TSS PERMIT(syspaudt) DSN(SYS3.CDS.) ACCESS(ALL)
TSS PERMIT(tstcaudt) DSN(SYS3.CDS.) ACCESS(ALL)
TSS PERMIT(icsfstc) DSN(SYS3.CDS.) ACCESS(ALL)

CCI: CCI-001499

Group ID (Vulid): V-255942
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-255942r881318_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-IC-000040
Rule Title: IBM Integrated Crypto Service Facility (ICSF) Started Task name is not properly identified / defined to the system ACP.
Legacy ID: SV-30591
Legacy ID: V-17452

Vulnerability Discussion: IBM Integrated Crypto Service Facility (ICSF) requires a started task that will be restricted to certain resources, datasets and other system functions. By defining the started task as a userid to the system ACP, It allows the ACP to control the access and authorized users that require these capabilities. Failure to properly control these capabilities, could compromise of the operating system environment, ACP, and customer data.

Check Content:

Review the IBM Integrated Crypto Service Facility (ICSF) STC/Batch ACID(s) for the following:

___ Is defined with Facility of STC and/or BATCH.

___ Is sourced to the INTRDR.

c) If all of the above are true this is not a finding

d) If any of the above is untrue this is a finding.

Fix Text: The Systems Programmer and IAO will ensure that the started task for IBM Integrated Crypto Service Facility (ICSF) Started Task(s) is properly Identified / defined to the System ACP.

If the product requires a Started Task, verify that it is properly defined to the System ACP with the proper attributes.

Most installation manuals will indicate how the Started Task is identified and any additional attributes that must be specified. Define the started task userid CSFSTART for IBM Integrated Crypto Service Facility (ICSF).

Example:

TSS CRE(CSFSTART) DEPT(Dept) NAME('ICSF STC') -
FAC(STC) PASSWORD(password,0) -
SOURCE(INTRDR)

CCI: CCI-000764

Group ID (Vulid): V-255943
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-255943r881321_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-IC-000050
Rule Title: IBM Integrated Crypto Service Facility (ICSF) Started task(s) must be properly defined to the Started Task Table ACID for Top Secret.
Legacy ID: V-17454
Legacy ID: SV-30580

Vulnerability Discussion: Access to product resources should be restricted to only those individuals responsible for the application connectivity and who have a requirement to access these resources. Improper control of product resources could potentially compromise the operating system, ACP, and customer data.

Check Content:
from the ISPF Command Shell enter

TSS LIST(STC)

If the IBM Integrated Crypto Service Facility (ICSF) started task(s) is (are) not defined in the TSS STC record this is a finding.

Fix Text: The IBM Integrated Crypto Service Facility (ICSF) system programmer and the IAO will ensure that a product's started task(s) is (are) properly identified and/or defined to the System ACP.

A unique ACID must be assigned for the IBM Integrated Crypto Service Facility (ICSF) started task(s) thru a corresponding STC table entry.

The following sample set of commands is shown here as a guideline:

TSS ADD(STC) PROCNAME(CSFSTART) ACID(CSFSTART)

CCI: CCI-000764

Group ID (Vulid): V-223985
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223985r877826_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-JS-000010
Rule Title: IBM z/OS JES2.** resource must be properly protected in the CA-TSS database.
Legacy ID: V-98677
Legacy ID: SV-107781

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Check Content:
From the ISPF Command Shell enter:
WHOOWNS OPERCMDS(JES2)
NOTE: JES2 is typically the name of the JES2 subsystem. Refer to the SUBSYS report and locate the entry with the description of PRIMARY JOB ENTRY SUBSYSTEM. The

SUBSYSTEM NAME of this entry is the name of the JES2 subsystem.

If the JES2. resource is not owned, or is owned inappropriately, in the OPERCMDS class, this is a finding.

Fix Text: The JES2. resource must be owned in the OPERCMDS class.

NOTE: JES2 is typically the name of the JES2 subsystem. Refer to the SUBSYS report and locate the entry with the description of PRIMARY JOB ENTRY SUBSYSTEM. The SUBSYSTEM NAME of this entry is the name of the JES2 subsystem.

Extended MCS support allows the installation to control the use of JES2 system commands through the ACP. These commands are subject to various types of potential abuse. For this reason, it is necessary to place restrictions on the JES2 system commands that can be entered by particular operators. To control access to JES2 system commands, the following recommendations will be applied when implementing security:

For Example:
The following command may be used to establish default protection for JES2 system commands defined to the OPERCMDS resource class:

TSS ADDTO(deptacid) OPERCMDS(JES2.)

CCI: CCI-000213

Group ID (Vulid): V-223986
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223986r877827_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-JS-000020
Rule Title: IBM z/OS RJE workstations and NJE nodes must be controlled in accordance with STIG requirements.
Legacy ID: V-98679
Legacy ID: SV-107783

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control

policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
Refer to SYS1.PARMLIB (JES2PARM)
For each node entry

If all JES2 defined NJE nodes and RJE workstations have a profile defined in the IBMFAC resource class, this is not a finding.

Notes: Nodename is the NAME parameter value specified on the NODE statement. Review the JES2 parameters for NJE node definitions by searching for "NODE(" in the report.
Workstation is RMTnnnn, where nnnn is the number on the RMT statement. Review the JES2 parameters for RJE workstation definitions by searching for "RMT(" in the report.
NJE. and RJE. definitions will force logonid and password protection of all NJE and RJE connections respectively. This method is acceptable in lieu of using discrete profiles.

If any JES2 defined NJE node or RJE workstation is not owned in the IBMFAC class, this is a finding.

Fix Text: Ensure associated USERIDs exist for all RJE/NJE sources and review the authorizations for these remote facilities. Develop a plan of action and implement the changes as required by the OS/390 STIG.

CCI: CCI-000213

Group ID (Vulid): V-223987
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223987r877828_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-JS-000030
Rule Title: IBM z/OS JES2 input sources must be controlled in accordance with the proper security requirements.
Legacy ID: V-98681
Legacy ID: SV-107785

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information

by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Check Content:
Refer the JES2PARM member of SYS1.PARMLIB
Review the following resources in the JESINPUT resource class:

NOTE: If any of the following are not defined within the JES2 parameters, the resource in the JESINPUT resource class does not have to be owned.
INTRDR (internal reader for batch jobs)
nodename (NJE node)
OFFn.* (spool offload receiver)
Rnnnn (RJE workstation)
RDRnn (local card reader)
STCINRDR (internal reader for started tasks)
TSUINRDR (internal reader for TSO logons)

Note 1: Nodename is the NAME parameter in the NODE statement. Review the NJE node definitions by searching for "NODE(" in the report.

Note 2: OFFn, where n is the number of the offload receiver. Review the spool offload receiver definitions by searching for "OFF(" in the report.

Note 3: Rnnnn, where nnnn is the number of the remote workstation. Review the RJE node definitions by searching for "RMT(" in the report.

Note 4: RDRnn, where nn is the number of the reader. Review the reader definitions by searching for "RDR(" in the report.

From the ISPF Command Shell enter:

TSS WHOOWNS JESINPUT(*)
If all of the resources above are owned by generic and/or fully qualified entries in the JESINPUT resource class, this is not a finding.

If any of the above resources are not owned, or are owned inappropriately, in the JESINPUT resource class, this is a finding.

Fix Text: Review the following resources in the JESINPUT resource class:

INTRDR (internal reader for batch jobs)
nodename (NJE node)
OFFn.* (spool offload receiver)
Rnnnn (RJE workstation)
RDRnn (local card reader)
STCINRDR (internal reader for started tasks)
TSUINRDR (internal reader for TSO logons)

Note: If any of the following are not defined within the JES2 parameters, the resource in the JESINPUT resource class does not have to be defined.

Note 1: Nodename is the NAME parameter in the NODE statement. Review the JES2 parameters for NJE node definitions by searching for "NODE(" in the report.

Note 2: OFFn, where n is the number of the offload receiver. Review the JES2 parameters for spool offload receiver definitions by searching for "OFF(" in the report.

Note 3: Rnnnn, where nnnn is the number of the remote workstation. Review the JES2 parameters for RJE node definitions by searching for "RMT(" in the report.

Note 4: RDRnn, where nn is the number of the reader. Review the JES2 parameters for reader definitions by searching for "RDR(" in the report.

Ensure all of the defined resources above are owned by generic and/or fully qualified entries in the JESINPUT resource class.

For Example:

The following commands may be used to establish default protection for resources defined to the JESINPUT resource class:

TSS ADDTO(deptacid) JESINPUT(OFFn.)

Grant read access to authorized users for each of the resources defined to the JESINPUT resource class.

The following is an example of granting operators with a profile ACID of jesopracid permission to restore jobs into any SPOOL off load processor after obtaining permission from the ISSO:

TSS PERMIT(jesopracid) JESINPUT(OFF*.) ACCESS(READ) ACTION(AUDIT)

The resource definition should be generic if all of the resources of the same type have identical access controls (e.g., if all off load receivers are equivalent).

CCI: CCI-000213

Group ID (Vulid): V-223988
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223988r877829_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-JS-000040
Rule Title: IBM z/OS JES2 input sources must be properly controlled.
Legacy ID: SV-107787
Legacy ID: V-98683

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Check Content:
From the ISPF Command Shell enter:
TSS WHOOWNS JESINPUT(*)
For each resource owned

If all of the TSS resources and/or generic equivalent identified above are defined with access restricted to the appropriate personnel, this is not a finding.

If any of the TSS resources and/or generic equivalent identified above are not defined with access restricted to the appropriate personnel, this is a finding.

From the ISPF Command Shell enter:
TSS LIST RDT(*)

If the JESINPT RESOURCE does not have DEFPROT as an attribute, this is a finding.

Fix Text: Configure access authorization for resources defined to the JESINPUT resource class to be restricted to the appropriate personnel.

Grant read access to authorized users for each of the following input sources:

INTRDR

nodename
OFFn.*
OFFn.JR
OFFn.SR
Rnnnn.RDm
RDRnn
STCINRDR
TSUINRDR and/or TSOINRDR

The resource definition will be generic if all of the resources of the same type have identical access controls (e.g., if all off load receivers are equivalent). The default access will be NONE except for sources that are permitted to submit jobs for all users. Those resources may be defined as either NONE or READ.

CCI: CCI-000213

Group ID (Vulid): V-223989
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223989r877830_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-JS-000050
Rule Title: IBM z/OS JES2 output devices must be controlled in accordance with the proper security requirements.
Legacy ID: SV-107789
Legacy ID: V-98685

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
Refer the JES2PARM member of SYS1.PARMLIB
Review the WRITER resource in the JESINPUT resource class:

NOTE: If the WRITER resource is not defined within the JES2 parameters, the resource in the JESINPUT resource class does not have to be owned.

From the ISPF Command Shell enter:
TSS WHOOWNS JESINPUT(WRITER)

If the WRITER resource is owned by generic and/or fully qualified entries in the JESINPUT resource class, this is not a finding.

Fix Text: Ensure the following items are in effect:

-The JES2. resource is owned in the WRITER resource class.

For Example:
The following command may be used to establish default protection for resources defined to the WRITER resource class:
TSS ADDTO(deptacid) WRITER(JES2.)

-The ownership of all WRITER resources is appropriate.

Grant read access to authorized users for each of the following WRITER resource class output destinations:

JES2.LOCAL.devicename
JES2.LOCAL.OFF*.JT
JES2.LOCAL.OFF*.ST
JES2.LOCAL.PRT*
JES2.LOCAL.PUN*
JES2.NJE.nodename
JES2.RJE.devicename

The following is an example of granting operators with a profile ACID of jesopracid permission to off load SYSOUT data sets into any SPOOL off load processor after obtaining permission from the ISSO:

TSS PERMIT(jesopracid) WRITER(JES2.LOCAL.OFF*.ST) -
ACCESS(READ) ACTION(AUDIT)

The resource definition should be generic if all of the resources of the same type have identical access controls (e.g., if all off load transmitters are equivalent).

CCI: CCI-000213

Group ID (Vulid): V-223990
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223990r877831_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-JS-000060
Rule Title: IBM z/OS JES2 output devices must be properly controlled for classified systems.
Legacy ID: V-98687
Legacy ID: SV-107791

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
If the Classification of the system is unclassified, this is not applicable.

From the ISPF Command Shell enter:
TSS WHOHAS WRITER(JES2.)

If the TSS WRITER resource or generic equivalent identified above is defined with access restricted to the appropriate personnel, this is not a finding.

If the TSS WRITER resource or generic equivalent identified above is not defined with access restricted to the appropriate personnel, this is a finding.

From the ISPF Command Shell enter:
TSS LIST RDT(*)

If the JESINPUT RESOURCE does not have DEFPROT as an attribute, this is a finding.

Fix Text: Configure access authorization for resources defined to the WRITER resource class to be restricted to the operators and system programmers on a classified system only.

Define resources in the ACP's respective WRITER class for each of the following output destinations:

JES2.LOCAL.devicename
JES2.LOCAL.OFFn.*
JES2.LOCAL.OFFn.JT
JES2.LOCAL.OFFn.ST
JES2.LOCAL.PRTn
JES2.LOCAL.PUNn
JES2.NJE.nodename
JES2.RJE.devicename

The resource definition will be generic if all of the resources of the same type have identical access controls (e.g., if all off load transmitters are equivalent). If all users are permitted to route output to a specific destination, the resource controlling it may be defined with a default access of either NONE or READ. Otherwise it will be defined with a default access of NONE.

CCI: CCI-000213

Group ID (Vulid): V-223991
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223991r877832_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-JS-000070
Rule Title: IBM z/OS JESSPOOL resources must be protected in accordance with security requirements.
Legacy ID: V-98689
Legacy ID: SV-107793

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
Refer the JES2PARM member of SYS1.PARMLIB. Review the JESSPOOL resource in the JESINPUT resource class:

NOTE: If the JESSPOOL resource is not defined within the JES2 parameters, the resource in the JESINPUT resource class does not have to be owned.

From the ISPF Command Shell enter:

TSS WHOOWNS JESINPUT(JESSPOOL)

If the JESSPOOL resource is owned by generic and/or fully qualified entries in the JESINPUT resource class, this is not a finding.

Fix Text: Review the JES2 parameters to determine the localnodeid by searching for OWNNODE in the NJEDEF statement, and then searching for NODE(nnnn) (where nnnn is the value specified by OWNNODE). The NAME parameter value specified on this NODE statement is the localnodeid.

The following command may be used to establish default protection for resources defined to the JESSPOOL resource class:

TSS ADDTO(deptacid) JESSPOOL(localnodeid.)

Due to the protection established with the previous command, the following command should be issued to ensure users are able to access their own spool data:

TSS PERMIT(ALL) JESSPOOL(localnodeid.%) ACCESS(ALL)

CCI: CCI-000213

Group ID (Vulid): V-223992
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223992r877833_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-JS-000080
Rule Title: IBM z/OS JESNEWS resources must be protected in accordance with security

requirements.
Legacy ID: SV-107795
Legacy ID: V-98691

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
From the ISPF Command Shell enter:
TSS WHOHAS OPERCMDS(JES2.)
NOTE: JES2 is typically the name of the JES2 subsystem. Refer to the SUBSYS report and locate the entry with the description of PRIMARY JOB ENTRY SUBSYSTEM. The SUBSYSTEM NAME of this entry is the name of the JES2 subsystem.

If access authorization to the JES2.UPDATE.JESNEWS resource in the OPERCMDS class restricts CONTROL access to the appropriate personnel (i.e., users responsible for maintaining the JES News data set) and all access is logged, this is not a finding.

Fix Text: Configure access authorization to the JES2.UPDATE.JESNEWS resource in the OPERCMDS class to restrict CONTROL access to the appropriate personnel (i.e., users responsible for maintaining the JES News data set) and ensure all access is logged.

NOTE: JES2 is typically the name of the JES2 subsystem. Refer to the SUBSYS report and locate the entry with the description of PRIMARY JOB ENTRY SUBSYSTEM. The SUBSYSTEM NAME of this entry is the name of the JES2 subsystem.

For example:

The following command example may be used to allow all valid TOP SECRET users read access to the JES News data set:

TSS PERMIT(ALL) JESSPOOL(localnodeid.jesid.$JESNEWS.*.*.JESNEWS) - ACCESS(READ)

The following is a sample command to allow production control personnel with a profile ACID of prodacid to update the JES News data set:

TSS PERMIT(prodacid) OPERCMDS(JES2.UPDATE.JESNEWS) - ACCESS(CONTROL) ACTION(AUDIT)

CCI: CCI-000213

Group ID (Vulid): V-223993
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223993r877834_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-JS-000090
Rule Title: IBM z/OS JESTRACE and/or SYSLOG resources must be protected in accordance with security requirements.
Legacy ID: SV-107797
Legacy ID: V-98693

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
From the ISPF Command Shell enter:
TSS WHOOWNS JESSPOOL(*)

If JESSPOOL localnodeid resource is not defined, this is a finding.

Enter
TSS WHOHAS JESSPOOL(localnodeid.)
Review the following resources defined to the JESSPOOL resource class:

localnodeid.JES2.$TRCLOG.taskid.*.JESTRACE
localnodeid.+MASTER+.SYSLOG.jobid.*.SYSLOG or
localnodeid.+BYPASS+.SYSLOG.jobid.-.SYSLOG

NOTE: These resource profiles may be more generic as long as they pertain directly to the JESTRACE and SYSLOG data sets. For example:

localnodeid.JES2.*.*.*.JESTRACE
localnodeid.+MASTER+.*.*.*.SYSLOG or
localnodeid.+BYPASS+.*.*.*.SYSLOG

NOTE: Review the JES2 parameters to determine the localnodeid by searching for OWNNODE in the NJEDEF statement, and then searching for NODE(nnnn) (where nnnn is the value specified by OWNNODE). The NAME parameter value specified on this NODE statement is the localnodeid. Another method is to issue the JES2 command $D NODE,NAME,OWNNODE=YES to obtain the NAME of the OWNNODE.

If the access authorization for the resources mentioned above is restricted to the following, this is not a finding.

-ACID(s) associated with external writer(s) can have complete access.

NOTE: An external writer is an STC that removes data sets from the JES spool. In this case, it is responsible for archiving the JESTRACE and SYSLOG data sets. The STC default name is XWTR and the external writer program is called IASXWR00.

-Systems personnel and security administrators responsible for diagnosing JES2 and z/OS problems can have complete access.

-Application Development and Application Support personnel responsible for diagnosing application problems can have READ access to the SYSLOG resource.

Fix Text: Configure the access authorization for resources defined to the JESTRACE and SYSLOG resources in the JESSPOOL resource class to be restricted to the appropriate personnel.

Review the following resources defined to the JESSPOOL resource class:

localnodeid.JES2.$TRCLOG.taskid.*.JESTRACE
localnodeid.+MASTER+.SYSLOG.jobid.*.SYSLOG or
localnodeid.+BYPASS+.SYSLOG.jobid.*.SYSLOG

NOTE: These resource profiles may be more generic as long as they pertain directly to the JESTRACE and SYSLOG data sets. For example:

localnodeid.JES2.$TRCLOG.
localnodeid.+MASTER+.SYSLOG. or
localnodeid.+BYPASS+.SYSLOG.

NOTE: Review the JES2 parameters to determine the localnodeid by searching for OWNNODE in the NJEDEF statement, and then searching for NODE(nnnn) (where nnnn is the value specified by OWNNODE). The NAME parameter value specified on this NODE statement is the localnodeid. Another method is to issue the JES2 command $D NODE,NAME,OWNNODE=YES to obtain the NAME of the OWNNODE.

Ensure that access authorization for the resources mentioned above is restricted to the following:

-ACID(s) associated with external writer(s) can have complete access.

NOTE: An external writer is a STC that removes data sets from the JES spool. In this case, it is responsible for archiving the JESTRACE and SYSLOG data sets. The STC default name is XWTR and the external writer program is called IASXWR00.

-Systems personnel and security administrators responsible for diagnosing JES2 and z/OS problems can have complete access.

-Application Development and Application Support personnel responsible for diagnosing application problems can have READ access to the SYSLOG resource.

For Example:

TSS ADD(dept-acid) JESSPOOL(localnodeid)

TSS PERMIT(<syspsmpl>) JESSPOOL(localnodeid.JES2.$TRCLOG.) ACCESS(ALL)
TSS PERMIT(<secasmpl>) JESSPOOL(localnodeid.JES2.$TRCLOG.) ACCESS(ALL)

TSS PERMIT(<syspsmpl>) JESSPOOL(localnodeid.+MASTER+.SYSLOG.) ACCESS(ALL)
TSS PERMIT(<secasmpl>) JESSPOOL(localnodeid.+MASTER+.SYSLOG.) ACCESS(ALL)
TSS PERMIT(<appdsmpl>) JESSPOOL(localnodeid.+MASTER+.SYSLOG.) ACCESS(READ)
TSS PERMIT(<appssmpl>) JESSPOOL(localnodeid.+MASTER+.SYSLOG.) ACCESS(READ)
or
TSS PERMIT(<syspsmpl>) JESSPOOL(localnodeid.+BYPASS+.SYSLOG.) ACCESS(ALL)
TSS PERMIT(<secasmpl>) JESSPOOL(localnodeid.+BYPASS+.SYSLOG.) ACCESS(ALL)
TSS PERMIT(<appdsmpl>) JESSPOOL(localnodeid.+BYPASS+.SYSLOG.) ACCESS(READ)
TSS PERMIT(<appssmpl>) JESSPOOL(localnodeid.+BYPASS+.SYSLOG.) ACCESS(READ)

CCI: CCI-000213

Group ID (Vulid): V-223994
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223994r877835_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-JS-000100
Rule Title: IBM z/OS JES2 spool resources must be controlled in accordance with security requirements.
Legacy ID: SV-107799
Legacy ID: V-98695

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
From the ISPF Command Shell enter:
TSS WHOHAS JESSPOOL(localnodeid.)

If the following guidance is true, this is not a finding.

Review the JESSPOOL report for resource permissions with the following naming convention. These permissions may be fully qualified, be specified as generic, or be specified with masking as indicated below:

localnodeid.useracid.jobname.jobid.dsnumber.name

localnodeid - The name of the node on which the SYSIN or SYSOUT data set currently resides.
useracid - The user ACID associated with the job. This is the user ACID TSS uses for validation purposes when the job runs.

jobname - The name that appears in the name field of the JOB statement.
jobid - The job number JES2 assigned to the job.
dsnumber - The unique data set number JES2 assigned to the spool data set. A D is the first character of this qualifier.
name - The name of the data set specified in the DSN= parameter of the DD statement. If the JCL did not specify DSN= on the DD statement that creates the spool data set, JES2 uses a question mark (?).

All users must have access to their own JESSPOOL resources. Permission can be granted by resource permission JESSPOOL(localnodeid.%.) ACCESS(ALL). This permission can be given to profiles, individual user, and/or the ALL record. Access to this resource does not require logging.

Ensure the following items are in effect:

The localnodeid. resource will be restricted to only system programmers, operators, and automated operations personnel, with access of ALL. All access will be logged. (localnodeid. resource includes all generic and/or masked permissions, example: localnodeid.**, localnodeid.*, etc.)

The JESSPOOL localnodeid.userid.jobname.jobid.dsnumber.name, whether generic and/or masked, can be made available to users, when approved by the ISSO. Access will be identified at the minimum access for the user to accomplish the users function. All access will be logged. An example is team members within a team, providing the capability to view, help, and/or debug other team member jobs/processes.

CSSMTP will be restricted to localnodeid.userid.jobname.jobid.dsnumber.name, whether generic and/or masked when approved by the ISSO. All access will be logged.

Spooling products users (CA-SPOOL, CA View, etc.) will be restricted to localnodeid.userid.jobname.jobid.dsnumber.name, whether generic and/or masked when approved by the ISSO. Logging of access is not required.

Fix Text: Configure the following items to be in effect for JESSPOOL resources. The JESSPOOL may have more restrictive security at the direction of the ISSO.

The JESSPOOL resources may be fully qualified, be specified as generic, or be specified with masking as indicated below:

localnodeid.userid.jobname.jobid.dsnumber.name

localnodeid - The name of the node on which the SYSIN or SYSOUT data set currently resides.
userid - The userid associated with the job. This is the userid used for validation purposes when the job runs.
jobname - The name that appears in the name field of the JOB statement.
jobid - The job number JES2 assigned to the job.

dsnumber - The unique data set number JES2 assigned to the spool data set. A D is the first character of this qualifier.
name - The name of the data set specified in the DSN= parameter of the DD statement. If the JCL did not specify DSN= on the DD statement that creates the spool data set, JES2 uses a question mark (?).

All users must have access to their own JESSPOOL resources. Permission can be granted by resource permission JESSPOOL(localnodeid.%.) ACCESS(ALL). This permission can be given to profiles, individual user, and/or the ALL record. Access to this resource does not require logging.

Example:
TSS ADDTO(deptacid) JESSPOOL(localnode.)
TSS PERMIT(ALL) JESSPOOL(localnode.%.) ACCESS(ALL)

The localnodeid. resource will be restricted to only system programmers, operators, and automated operations personnel, with access of ALL. All access will be logged. (localnodeid. resource includes all generic and/or masked permissions, example: localnodeid.**, localnodeid.*, etc.)

Example:
TSS PERMIT(syspsmpl) JESSPOOL(localnodeid.) ACCESS(ALL) ACTION(AUDIT)

The JESSPOOL localnodeid.userid.jobname.jobid.dsnumber.name, whether generic and/or masked, can be made available to users, when approved by the ISSO. Access will be identified at the minimum access for the user to accomplish the users function. All access will be logged. An example is team members within a team, providing the capability to view, help, and/or debug other team member jobs/processes. If frequent situations occur where users working on a common project require selective access to each other's jobs, then the installation may delegate to the individual users the authority to grant access, but only with the approval of the ISSO.

Example:
TSS PERMIT(Project1-profile) JESSPOOL(localnodeid.UMO) ACCESS(ALL)

If IBM's SDSF product is installed on the system, resources defined to the JESSPOOL resource class control functions related to jobs, output groups, and SYSIN/SYSOUT data sets on various SDSF panels.

CSSMTP will not be granted to the JESSPOOL resource of the high level "node." or "localnodeid.". CSSMTP can have access to the specific approved JESSPOOL resources, minimally qualified to the "node.userid." and all access will be logged. This will ensure system records who (userid) sent traffic to CSSMTP, when and what job/process.

Spooling products users (CA-SPOOL, CA View, etc.) will be restricted to localnodeid.userid.jobname.jobid.dsnumber.name, whether generic and/or masked when approved by the ISSO. Logging of access is not required.

The ISSO will review JESSPOOL resource rules. If a rule has been determined not to have been used within the last two years, the rule will be removed.

CCI: CCI-000213

Group ID (Vulid): V-223995
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223995r877836_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-JS-000110
Rule Title: IBM z/OS JES2 system commands must be protected in accordance with security requirements.
Legacy ID: SV-107801
Legacy ID: V-98697

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
From the ISPF Command Shell enter:
TSS WHOHAS OPERCMDS(JES2.)

If the JES2.** resource is defined to the OPERCMDS class with an access of NONE and all access is logged, this is not a finding.

If access to JES2 system commands defined in the IBM z/OS JES2 commands is restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users), this is not a finding.

NOTE: Use the GROUP category specified in the table referenced above as a guideline to determine appropriate personnel access to system commands.

Fix Text: Extended MCS support allows the installation to control the use of JES2 system commands through the ESM. These commands are subject to various types of potential abuse. For this reason, it is necessary to place restrictions on the JES2 system commands that can be entered by particular operators.

Some commands are particularly dangerous and should only be used when less drastic options have been exhausted. Misuse of these commands can create a situation in which the only recovery is an IPL.

To control access to JES2 system commands, apply the following:
implementing security:

Define the JES2.** resource in the OPERCMDS class with an access of NONE and all access is logged.

Define the JES2 system commands as specified in the IBM z/OS JES2 Commands to be restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users), as determined in the documented site Security Plan.

Define the JES2 system commands with proper logging as determined in the documented site Security Plan.
Note: Display commands and others as deemed by the site IAW site security plan may be allowed for all users with no logging.

Build a command file based on the referenced JES2 Command Table. A sample of the commands in the command file is provided here:

RDEF OPERCMDS JES2.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('REQUIRED BY SRR PDI ZJES0052')

RDEF OPERCMDS JES2.<command>.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('REQUIRED BY SRR PDI ZJES0052')
PE JES2.<command>.** CL(OPERCMDS) ID(<syspsmpl>) ACC(U)

SETR RACL(OPERCMDS) REF

CCI: CCI-000213

Group ID (Vulid): V-223996
Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223996r877837_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-JS-000120
Rule Title: IBM z/OS Surrogate users must be controlled in accordance with proper security requirements.
Legacy ID: SV-107803
Legacy ID: V-98699

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000326-GPOS-00126

Check Content:
From the ISPF Command Shell enter:
TSS LIST(ACIDS) DATA(XA)

If no XA ACID entries exist in the above reports, this is not applicable.

For each ACID identified in the XA ACID entries, if the following items are true regarding ACID permissions, this is not a finding.

-ACID permission (XA ACID) is logged (ACTION = AUDIT), only for Privileged USERIDS (MASTER, SCA, DCA, VCA, ZCA) if they are XAUTH; at the discretion of the ISSM/ISSO scheduling tasks may be exempted from logging.
-Access authorization is restricted to scheduling tools, started tasks or other system applications required for running production jobs.
-Other users may have minimal access required for running production jobs with documentation properly approved and filed with the site security official (ISSM or equivalent).

Fix Text: For each ACID identified in the XA ACID entries, ensure the following items are in

effect regarding ACID permissions:

-ACID permission (XA ACID) is logged (ACTION = AUDIT), at the discretion of the ISSM/ISSO scheduling tasks may be exempted from logging.
-ACID permission (XA ACID) is logged (ACTION = AUDIT), for Privileged users (MSCA, SCA, DCA, VCA, ZCA).
-Access authorization is restricted to scheduling tools, started tasks, or other system applications required for running production jobs.

Other users may have minimal access required for running production jobs with documentation properly approved and filed with the site security official (ISSM or equivalent).

Consider the following recommendations when implementing security for Cross-Authorized ACIDs:

Keep ACID cross authorization of ACIDs outside of those granted to the scheduling software to a minimum number of individuals.

The simplest configuration is to have no ACID Cross Authorization except for the appropriate Scheduling task/software for production scheduling purposes as documented.

Temporary Cross Authorization of the production batch ACID to the scheduling tasks may be allowed for a period for testing by the appropriate specific production Support Team members. Authorization, eligibility, and test period is determined by site policy.

Access authorization is restricted to the minimum number of personnel required for running production jobs. However, ACID Cross Authorization usage must not become the default for all jobs submitted by individual userids (i.e., system programmer will use their assigned individual userids for software installation, duties, whereas a Cross-Authorized ACID would normally be utilized for scheduled batch production only and as such must normally be limited to the scheduling task such as CONTROLM) and not granted as a normal daily basis to individual users.

Grant access to the user ACID for each cross-authorized ACID required:

For Example:
TSS PERMIT(ACID) ACID(Cross-Authorized ACID) ACTION(AUDIT)

For production ACIDs being used by CONTROLM:
TSS PER(CONTROLM)ACID(production user ACID)

CCI: CCI-000213

CCI: CCI-002233

Group ID (Vulid): V-223997
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-223997r877838_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000010
Rule Title: Duplicated IBM z/OS sensitive utilities and/or programs must not exist in APF libraries.
Legacy ID: SV-107805
Legacy ID: V-98701

Vulnerability Discussion: Removal of unneeded or non-secure functions, ports, protocols, and services mitigate the risk of unauthorized connection of devices, unauthorized transfer of information, or other exploitation of these resources.

Check Content:
From an ISPF Command line enter:
TSO ISRDDN APF

An APF List results. On the Command line enter:
DUPlicates (Make sure there is appropriate access. If there is not, you may receive insufficient access errors.)

If any of the list of Sensitive Utilities exist in the duplicate APF modules returned, this is a finding.

The following list contains Sensitive Utilities that will be checked.

AHLGTF AMASPZAP AMAZAP AMDIOCP AMZIOCP
BLSROPTR CSQJU003 CSQJU004 CSQUCVX CSQUTIL
CSQ1LOGP DEBE DITTO FDRZAPOP GIMSMP
HHLGTF ICKDSF ICPIOCP IDCSC01 IEHINITT
IFASMFDP IGWSPZAP IHLGTF IMASPZAP IND$FILE
IOPIOCP IXPIOCP IYPIOCP IZPIOCP WHOIS
L052INIT TMSCOPY TMSFORMT TMSLBLPR TMSMULV
TMSREMOV TMSTPNIT TMSUDSNB

Fix Text: Review and ensure that duplicate sensitive utility(ies) and/or program(s) do not exist in APF-authorized libraries. Identify all versions of the sensitive utilities contained in APF-authorized libraries listed in the above check. In cases where duplicates exist, ensure no exposure has been created and written justification has been filed with the ISSO.

Comparisons among all the APF libraries will be done to ensure that an exposure is not created

by the existence of identically named modules. Address any sensitive utility concerns so that the function can be restricted as required.

CCI: CCI-000381

Group ID (Vulid): V-223998
Group Title: SRG-OS-000004-GPOS-00004
Rule ID: SV-223998r877839_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000020
Rule Title: IBM z/OS required SMF data record types must be collected.
Legacy ID: SV-107807
Legacy ID: V-98703

Vulnerability Discussion: Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to create an account. Auditing account creation actions provides logging that can be used for forensic purposes.

To address access requirements, many operating systems may be integrated with enterprise level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000040-GPOS-00018, SRG-OS-000041-GPOS-00019, SRG-OS-000042-GPOS-00021, SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000462-GPOS-00206, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209, SRG-OS-000466-GPOS-00210, SRG-OS-000467-GPOS-00211, SRG-OS-000468-GPOS-00212, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000471-GPOS-00215, SRG-OS-000471-GPOS-00216, SRG-OS-000472-GPOS-00217, SRG-OS-000473-GPOS-00218, SRG-OS-000474-GPOS-00219, SRG-OS-000475-GPOS-00220, SRG-OS-000476-GPOS-00221, SRG-OS-000477-GPOS-00222, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000255-GPOS-00096, SRG-OS-000365-GPOS-00152, SRG-OS-000348-GPOS-00136, SRG-OS-000303-GPOS-00120, SRG-OS-000327-GPOS-00127, SRG-OS-000392-GPOS-00172

Check Content:
Refer to IEASYS00 member in SYS1.PARMLIB Concatenation. Determine proper SMFPRMxx member.

If all of the required SMF record types identified below are collected, this is not a finding.

IBM SMF Records to be collected at a minimum:

0 (00) - IPL
6 (06) - External Writer/ JES Output Writer/ Print Services Facility (PSF)
7 (07) - [SMF] Data Lost
14 (0E) - INPUT or RDBACK Data Set Activity
15 (0F) - OUTPUT, UPDAT, INOUT, or OUTIN Data Set Activity
17 (11) - Scratch Data Set Status
18 (12) - Rename Non-VSAM Data Set Status
24 (18) - JES2 Spool Offload
25 (19) - JES3 Device Allocation
26 (1A) - JES Job Purge
30 (1E) - Common Address Space Work
32 (20) - TSO/E User Work Accounting
41 (29) - DIV Objects and VLF Statistics
42 (2A) - DFSMS statistics and configuration
43 (2B) - JES Start
45 (2D) - JES Withdrawal/Stop
47 (2F) - JES SIGNON/Start Line (BSC)/LOGON
48 (30) - JES SIGNOFF/Stop Line (BSC)/LOGOFF
49 (31) - JES Integrity
52 (34) - JES2 LOGON/Start Line (SNA)
53 (35) - JES2 LOGOFF/Stop Line (SNA)
54 (36) - JES2 Integrity (SNA)
55 (37) - JES2 Network SIGNON
56 (38) - JES2 Network Integrity
57 (39) - JES2 Network SYSOUT Transmission
58 (3A) - JES2 Network SIGNOFF
60 (3C) - VSAM Volume Data Set Updated
61 (3D) - Integrated Catalog Facility Define Activity
62 (3E) - VSAM Component or Cluster Opened
64 (40) - VSAM Component or Cluster Status
65 (41) - Integrated Catalog Facility Delete Activity
66 (42) - Integrated Catalog Facility Alter Activity
80 (50) - RACF/TOP SECRET Processing
81 (51) - RACF Initialization
82 (52) - ICSF Statistics
83 (53) - RACF Audit Record For Data Sets
90 (5A) - System Status
92 (5C) except subtypes 10, 11 - OpenMVS File System Activity
102 (66) - DATABASE 2 Performance
103 (67) - IBM HTTP Server
110 (6E) - CICS/ESA Statistics
118 (76) - TCP/IP Statistics
119 (77) - TCP/IP Statistics

199 (C7) - TSOMON
230 (E6) - ACF2 or as specified in ACFFDR (vendor-supplied default is 230)
231 (E7) - TSS logs security events under this record type

Fix Text: Ensure that SMF recording options are consistent with those outlined below.

IBM SMF Records to be collected at a minimum:

0 (00) - IPL
6 (06) - External Writer/ JES Output Writer/ Print Services Facility (PSF)
7 (07) - [SMF] Data Lost
14 (0E) - INPUT or RDBACK Data Set Activity
15 (0F) - OUTPUT, UPDAT, INOUT, or OUTIN Data Set Activity
17 (11) - Scratch Data Set Status
18 (12) - Rename Non-VSAM Data Set Status
24 (18) - JES2 Spool Offload
25 (19) - JES3 Device Allocation
26 (1A) - JES Job Purge
30 (1E) - Common Address Space Work
32 (20) - TSO/E User Work Accounting
41 (29) - DIV Objects and VLF Statistics
42 (2A) - DFSMS statistics and configuration
43 (2B) - JES Start
45 (2D) - JES Withdrawal/Stop
47 (2F) - JES SIGNON/Start Line (BSC)/LOGON
48 (30) - JES SIGNOFF/Stop Line (BSC)/LOGOFF
49 (31) - JES Integrity
52 (34) - JES2 LOGON/Start Line (SNA)
53 (35) - JES2 LOGOFF/Stop Line (SNA)
54 (36) - JES2 Integrity (SNA)
55 (37) - JES2 Network SIGNON
56 (38) - JES2 Network Integrity
57 (39) - JES2 Network SYSOUT Transmission
58 (3A) - JES2 Network SIGNOFF
60 (3C) - VSAM Volume Data Set Updated
61 (3D) - Integrated Catalog Facility Define Activity
62 (3E) - VSAM Component or Cluster Opened
64 (40) - VSAM Component or Cluster Status
65 (41) - Integrated Catalog Facility Delete Activity
66 (42) - Integrated Catalog Facility Alter Activity
80 (50) - RACF/TOP SECRET Processing
81 (51) - RACF Initialization
82 (52) - ICSF Statistics
83 (53) - RACF Audit Record For Data Sets
90 (5A) - System Status
92 (5C) except subtypes 10, 11 - OpenMVS File System Activity

102 (66) - DATABASE 2 Performance
103 (67) - IBM HTTP Server
110 (6E) - CICS/ESA Statistics
118 (76) - TCP/IP Statistics
119 (77) - TCP/IP Statistics
199 (C7) - TSOMON
230 (E6) - ACF2 or as specified in ACFFDR (vendor-supplied default is 230)
231 (E7) - TSS logs security events under this record type

CCI: CCI-000018

CCI: CCI-000130

CCI: CCI-000131

CCI: CCI-000132

CCI: CCI-000133

CCI: CCI-000134

CCI: CCI-000135

CCI: CCI-000172

CCI: CCI-001403

CCI: CCI-001404

CCI: CCI-001405

CCI: CCI-001487

CCI: CCI-001814

CCI: CCI-001875

CCI: CCI-002130

CCI: CCI-002234

CCI: CCI-002884

Group ID (Vulid): V-223999
Group Title: SRG-OS-000029-GPOS-00010
Rule ID: SV-223999r877840_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000030
Rule Title: IBM z/OS Session manager must properly configure wait time limits.
Legacy ID: V-98705
Legacy ID: SV-107809

Vulnerability Discussion: A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Check Content:
If the session manager in use initiates a session lock after a 15-minute period of inactivity for all connection types, this is not a finding.

Fix Text: Configure the session manager in use to initiate a session lock after a 15-minute period of inactivity for all connection types.

CCI: CCI-000057

Group ID (Vulid): V-224000
Group Title: SRG-OS-000032-GPOS-00013
Rule ID: SV-224000r877841_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000040
Rule Title: The IBM z/OS BPX.SMF resource must be properly configured.
Legacy ID: SV-107811
Legacy ID: V-98707

Vulnerability Discussion: Remote access services, such as those providing remote access to network devices and information systems, which lack automated monitoring capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Automated monitoring of remote access sessions allows organizations to detect cyberattacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote access capabilities, such as Remote Desktop Protocol (RDP), on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Check Content:
Review the FACILITY resource class for BPX.SMF.

If the RACF rules are as follows, this is not a finding.

BPX.SMF.119.94 - READ allowed for users running the ssh, sftp, or scp client commands.
BPX.SMF.119.96 - READ allowed for users running the scp or sftp-server server commands.
BPX.SMF.119.97 - READ allowed for users running the scp or sftp client commands.

The following profile grants the permitted users the authority to write or test for any SMF record being recorded. Access should be permitted as follows:
BPX.SMF - READ access only when documented and justified in Site Security Plan.
Documentation should include a reason why a more specific profile is not acceptable.

Fix Text: Configure Facility resource class for BPX.SMF as follows:

BPX.SMF.119.94 - READ allowed for users running the ssh, sftp, or scp client commands.
BPX.SMF.119.96 - READ allowed for users running the scp or sftp-server server commands.
BPX.SMF.119.97 - READ allowed for users running the scp or sftp client commands.

The following profile grants the permitted users the authority to write or test for any SMF record being recorded. Access should be permitted as follows:
BPX.SMF - READ access only when documented and justified in Site Security Plan.
Documentation should include a reason why a more specific profile is not acceptable.

CCI: CCI-000067

Group ID (Vulid): V-224001
Group Title: SRG-OS-000038-GPOS-00016
Rule ID: SV-224001r877842_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000050
Rule Title: IBM z/OS must specify SMF data options to ensure appropriate activation.
Legacy ID: SV-107813
Legacy ID: V-98709

Vulnerability Discussion: Without establishing when events occurred, it is impossible to establish, correlate, and investigate the events leading up to an outage or attack.

In order to compile an accurate risk assessment and provide forensic analysis, it is essential for security personnel to know when events occurred (date and time).

Associating event types with detected events in the operating system audit logs provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured operating system.

Satisfies: SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000040-GPOS-00018, SRG-OS-000041-GPOS-00019, SRG-OS-000042-GPOS-00021, SRG-OS-000254-GPOS-00095, SRG-OS-000269-GPOS-00103, SRG-OS-000368-GPOS-00154

Check Content:
Refer to IEASYS00 member in SYS1.PARMLIB Concatenation. Determine proper SMFPRMxx member.

SUBSYS(STC,EXITS(IEFU29,IEFU83,IEFU84,IEFUJP,IEFUSO),
INTERVAL(SMF,SYNC),NODETAIL)

If the SMF collection options are specified as stated below with exception of those specified in the above NOTEs, this is not a finding.

The settings for several parameters are critical to the collection process:

ACTIVE Activates the collection of SMF data.

MAXDORM(0500) Specifies the amount of real time that SMF allows data to remain in an SMF buffer before it is written to a recording data set. Value is site defined.

SID Specifies the system ID to be recorded in all SMF records.

SYS(DETAIL) Controls the level of detail recorded.

SYS(INTERVAL) Ensures the periodic recording of data for long running jobs.

SYS Specifies the types and sub types of SMF records that are to be collected. SYS(TYPE) indicates that the supplied list is inclusive (i.e., specifies the record types to be collected). Record types not listed are not collected. SYS(NOTYPE) indicates that the supplied list is exclusive (i.e., specifies those record types not to be collected). Record types listed are not collected. The site may use either form of this parameter to specify SMF record type collection. However, at a minimum, all record types are listed.

Fix Text: Ensure that collection options for SMF Data are consistent with options specified below.

Review all SMF recording specifications found in SMFPRMxx members. Ensure that SMF recording options used are consistent with those outlined below.

The settings for several parameters are critical to the collection process:

ACTIVE Activates the collection of SMF data.

MAXDORM(mmss) Specifies the amount of real time that SMF allows data to remain in an SMF buffer before it is written to a recording data set. Use the MAXDORM parameter to minimize the amount of data lost because of system failure. This value is site determined and should be carefully configured.

SID Specifies the system ID to be recorded in all SMF records.

SYS(DETAIL) Controls the level of detail recorded.

SYS(INTERVAL) Ensures the periodic recording of data for long running jobs.

SYS Specifies the types and sub types of SMF records that are to be collected. SYS(TYPE) indicates that the supplied list is inclusive (i.e., specifies the record types to be collected). Record types not listed are not collected. SYS(NOTYPE) indicates that the supplied list is exclusive (i.e., specifies those record types not to be collected). Record types not listed are not collected. The site may use either form of this parameter to specify SMF record type collection. However, at a minimum all record types are listed.

CCI: CCI-000131

CCI: CCI-000132

CCI: CCI-000133

CCI: CCI-000134

CCI: CCI-000135

CCI: CCI-001464

CCI: CCI-001665

CCI: CCI-001764

Group ID (Vulid): V-224002
Group Title: SRG-OS-000046-GPOS-00022
Rule ID: SV-224002r877843_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000060
Rule Title: IBM z/OS BUFUSEWARN in the SMFPRMxx must be properly set.
Legacy ID: SV-107815
Legacy ID: V-98711

Vulnerability Discussion: It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Check Content:
Refer to IEASYS00 member in SYS1.PARMLIB Concatenation. Determine proper SMFPRMxx member in SYS1.PARMLIB.

If BUFUSEWARN is set for "75" (75%) or less, this is not a finding.

Fix Text: Configure the BUFUSEWARN statement in SMFPRMxx to "75" (75%) or less.

CCI: CCI-000139

Group ID (Vulid): V-224003
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-224003r877844_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000070
Rule Title: IBM z/OS PASSWORD data set and OS passwords must not be used.
Legacy ID: V-98713
Legacy ID: SV-107817

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Check Content:
Ask the system administrator to determine if the system PASSWORD data set and OS passwords are being used.

If, based on the information provided, it can be determined that the system PASSWORD data set and OS passwords are not used, this is not a finding.

If it is evident that OS passwords are utilized, this is a finding.

Fix Text: System programmers will ensure that the old OS Password Protection is not used and any data protected by the old OS Password technology is removed and protection is replaced by the ACP.

Review the contents of the PASSWORD data set. Ensure that any protections it provides are provided by the ACP and delete the PASSWORD data set.

Access to data sets on z/OS systems can be protected using the OS password capability of MVS. This capability has been available in MVS for many years, and its use is commonly found in data centers. Since the advent of ACPs, the use of OS passwords for file protection has diminished, and is commonly considered archaic and of little use. The use of z/OS passwords is not supported by all the ACPs.

CCI: CCI-000366

Group ID (Vulid): V-224004
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-224004r877845_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000080
Rule Title: The CA-TSS database must be on a separate physical volume from its backup and recovery data sets.
Legacy ID: V-98715
Legacy ID: SV-107819

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Check Content:
Refer to the System proclibs for the TSS STC.

If the Security database is located on the same volume as either the backup, Alternate or Recovery file, this is a finding.

Fix Text: Configure the placement of ESM files are on a separate volume from its backup and recovery data sets to provide backup and recovery in the event of physical damage to a volume.

Identify the ESM database(s), backup database(s), and recovery data set(s). Develop a plan to keep these data sets on different physical volumes. Implement the movement of these critical ESM files.

File location is an often overlooked factor in system integrity. It is important to ensure that the effects of hardware failures on system integrity and availability are minimized. Avoid collocation of files such as primary and alternate databases. For example, the loss of the physical volume containing the ESM database should not also cause the loss of the ESM backup database as a result of their collocation. Files that will be segregated from each other on separate physical volumes include, but are not limited to, the ESM database and its alternate or backup file.

CCI: CCI-000366

Group ID (Vulid): V-224005
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-224005r877846_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000090
Rule Title: The CA-TSS database must be backed up on a scheduled basis.
Legacy ID: V-98717
Legacy ID: SV-107821

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Check Content:

Refer to the TSS Proclib PARMFILE DD to determine the PARM member.

If the BACKUP is missing or coded with blank or OFF this is a finding.

Note: If the security data base is shared only one of the systems is required to configure the BACKUP option in the PARMFILE. Determine that the option is properly coded on one of the systems that share the security database.

From the ISPF Command Shell enter:
TSS MODIFY(Status)

If the backup parameter is active with a valid time this is not a finding.

Fix Text: Configure the TSS PARMLIB BACKUP parameter to include BACKUP statement with a valid time. Additionally, configure the BACKUP parameter in the TSS Parmfile to include BACKUP statement with a valid time for nightly backups.

CCI: CCI-000366

Group ID (Vulid): V-224006
Group Title: SRG-OS-000480-GPOS-00232
Rule ID: SV-224006r877847_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000100
Rule Title: The IBM z/OS Policy Agent must be configured to deny-all, allow-by-exception firewall policy for allowing connections to other systems.
Legacy ID: V-98719
Legacy ID: SV-107823

Vulnerability Discussion: Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Check Content:
Examine the policy agent policy statements. If it can be determined that the policy agent employs a deny-all, allow-by exception firewall policy for allowing connections to other systems this is not a finding.

Fix Text: Develop a policy application and policy agent to employ a deny-all, allow-by-exception firewall policy for allowing connections to other systems.

CCI: CCI-000366

CCI: CCI-002080

Group ID (Vulid): V-224007
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-224007r877848_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000110
Rule Title: IBM z/OS must not have Inaccessible APF libraries defined.
Legacy ID: V-98723
Legacy ID: SV-107827

Vulnerability Discussion: It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software, not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Check Content:
Refer to IEASYS00 member in SYS1.PARMLIB Concatenation. Determine proper APF and/or PROG member.
Examine each entry and verify that it exists on the specified volume.

If inaccessible APF libraries exist, this is a finding.

ISRDDN APF

Fix Text: Review the entire list of APF authorized libraries and remove those that are no longer valid designations.

CCI: CCI-000381

Group ID (Vulid): V-224008
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-224008r877849_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000120
Rule Title: IBM z/OS inapplicable PPT entries must be invalidated.
Legacy ID: SV-107829
Legacy ID: V-98725

Vulnerability Discussion: It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software, not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Check Content:
Review program entries in the IBM Program Properties Table (PPT). You may use a third-party product to examine these entries; however, to determine program entries, issue the following command from an ISPF command line:
TSO ISRDDN LOAD IEFSDPPT
Press Enter.

Interpret the display as follows:
Examine contents at offset 8
Hex 'x2' - Bypass Password Protection
Hex 'x3' - Bypass Password Protection
Hex 'x4' - No data set Integrity
Hex 'x5' - No data set Integrity
Hex 'x6' - Both
Hex 'x7' - Both
Determine Privilege Key at offset 9. A value of hex '70' or less indicates an elevated privilege.

For each module identified in the "eyecatcher" that has BYPASS Password Protection, No data set Integrity, an elevated Privilege Key, or any combination thereof, determine if there is a valid loaded module. Again, you may use a third-party product; otherwise, execute the following steps:
From an ISPF command line
TSO ISRDDN LOAD <privileged module>
Press Enter.

If the return message is "Load Failed", make sure there is an entry in PARMLIB member SCHEDxx that revokes the excessive privilege.

If this is not true, this is a finding.

Fix Text: Review the PPT and define all entries associated with nonexistent or inapplicable modules as invalidated. Nullify the invalid IEFSDPPT entry by ensuring that there is a corresponding SCHED entry, which confers no special attributes.

Use the following recommendations and techniques to provide protection for the PPT:

Review the IEFSDPPT module and all programs that IBM has, by default, placed in the PPT to validate their applicability to the execution system. Refer to the IBM z/OS MVS Initialization and Tuning Reference documentation for the version and release of z/OS installed at the individual site for the actual contents of the default IEFSDPPT.

Modules for products not in use on the system will have their special privileges explicitly revoked. Do this by placing a PPT entry for each module in the SYS1.PARMLIB(SCHEDxx) member, specifying no special privileges. The PPT entry for each overridden program will be in the following format, accepting the default (unprivileged) values for the sub parameters:

PPT PGMNAME(<program name>)

Assemble documentation regarding these PPT entries, and the ISSO will keep it on file. Include the following in the documentation:

-The product and release for which the PPT entry was made
-The last date this entry was reviewed to authenticate status
-The reason the module's privileges are being revoked

CCI: CCI-000381

Group ID (Vulid): V-224009
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-224009r877850_rule
Severity: CAT II

Rule Version (STIG-ID): TSS0-OS-000130
Rule Title: IBM z/OS LNKAUTH=APFTAB must be specified in the IEASYSxx member(s) in the currently active parmlib data set(s).
Legacy ID: SV-107831
Legacy ID: V-98727

Vulnerability Discussion: It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software, not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Check Content:
Refer to IEASYS00 member in SYS1.PARMLIB Concatenation.

If "LNKAUTH=APFTAB" is not specified, this is a finding.

Fix Text: Configure LNKAUTH=APFTAB in the IEASYS00 member of PARMLIB.

CCI: CCI-000381

Group ID (Vulid): V-224010
Group Title: SRG-OS-000138-GPOS-00069
Rule ID: SV-224010r877851_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000140
Rule Title: IBM z/OS sensitive and critical system data sets must not exist on shared DASD.
Legacy ID: SV-107833
Legacy ID: V-98729

Vulnerability Discussion: Preventing unauthorized information transfers mitigates the risk of information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources

(e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

This requirement generally applies to the design of an information technology product, but it can also apply to the configuration of particular information system components that are, or use, such products. This can be verified by acceptance/validation processes in DoD or other government agencies.

There may be shared resources with configurable protections (e.g., files in storage) that may be assessed on specific information system components.

Check Content:
Check HMC, VM, and z/OS on how to validate and determine a DASD volume(s) is shared.

Note: In VM issue the command "QUEUE DASD SYSTEM" this display will show shared volume(s) and indicates the number of systems sharing the volume.

Validate all machines that require access to these shared volume(s) have the volume(s) mounted.

Obtain a map or list VTOC of the shared volume(s).

Check if shared volume(s) contain any critical or sensitive data sets.

Identify shared and critical or sensitive data sets on the system being audited. These data sets can be APF, LINKLIST, LPA, Catalogs, etc, as well as product data sets.

If all of the critical or sensitive data sets identified on shared volume(s) are protected and justified to be on shared volume(s), this is not a finding.

List critical or sensitive data sets are possible security breaches, if not justified and not protected on systems having access to the data set(s) and on shared volume(s).

Fix Text: Configure all identified volumes of shared DASD to be valid within the following.

HMC
VM
z/OS

If the shared volume(s) are valid and systems having access to these shared volume(s) are valid, map disk/VTOC list to obtain data sets on the shared volume(s). From this list obtain a list of sensitive and critical system data sets that are found on the shared volume(s). Ensure that the data sets are justified to be shared on the system and to reside on the shared volume(s).

The ISSO will review all access requirements to validate that sensitive and critical system data

sets are protected from unauthorized access across all systems that have access to the shared volume(s). Protecting the data set(s) whether the data set(s) are used or not used on the systems that have the shared volume(s) available to them.

CCI: CCI-001090

Group ID (Vulid): V-224011
Group Title: SRG-OS-000142-GPOS-00071
Rule ID: SV-224011r877852_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000150
Rule Title: The IBM z/OS Policy Agent must contain a policy that manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service (DoS) attacks.
Legacy ID: SV-107835
Legacy ID: V-98731

Vulnerability Discussion: DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

Check Content:
Examine the Policy Agent policy statements.

If it can be determined that there are policy statements that manages excess capacity, this is not a finding.

Fix Text: Develop Policy application and Policy agent to manage excess capacity.

CCI: CCI-001095

Group ID (Vulid): V-224013
Group Title: SRG-OS-000274-GPOS-00104
Rule ID: SV-224013r877853_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000170
Rule Title: The IBM z/OS System Administrator must develop a process to notify appropriate personnel when accounts are created.
Legacy ID: V-98735
Legacy ID: SV-107839

Vulnerability Discussion: Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to create a new account. Notification of account creation is one method for mitigating this risk. A comprehensive account management process will ensure an audit trail which documents the creation of operating system user accounts and notifies administrators and ISSOs that it exists. Such a process greatly reduces the risk that accounts will be surreptitiously created and provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Check Content:
Ask the system Administrator for the documented process to notify appropriate personnel when accounts are created.

If there is no documented process, this is a finding.

Fix Text: Develop a documented process to notify appropriate personnel when accounts are created.

CCI: CCI-001683

Group ID (Vulid): V-224014
Group Title: SRG-OS-000275-GPOS-00105
Rule ID: SV-224014r877854_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000180
Rule Title: The IBM z/OS System Administrator must develop a process to notify appropriate personnel when accounts are modified.
Legacy ID: V-98737
Legacy ID: SV-107841

Vulnerability Discussion: Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to create a new account. Notification of account creation is one method for mitigating this risk. A comprehensive account management process will ensure an audit trail which documents the creation of operating system user accounts and notifies administrators and ISSOs that it exists. Such a process greatly reduces the risk that accounts will be surreptitiously created and provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Check Content:
Ask the system Administrator for the documented process to notify appropriate personnel when accounts are modified.

If there is no documented process, this is a finding.

Fix Text: Develop a documented process to notify appropriate personnel when accounts are modified.

CCI: CCI-001684

Group ID (Vulid): V-224015
Group Title: SRG-OS-000276-GPOS-00106
Rule ID: SV-224015r877855_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000190
Rule Title: The IBM z/OS System Administrator must develop a process to notify appropriate personnel when accounts are deleted.
Legacy ID: V-98739
Legacy ID: SV-107843

Vulnerability Discussion: When operating system accounts are disabled, user accessibility is affected. Accounts are utilized for identifying individual operating system users or for identifying the operating system processes themselves. Sending notification of account disabling events to the system administrator and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that operating system accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Check Content:
Ask the system Administrator for the documented process to notify appropriate personnel when accounts are deleted.

If there is no documented process, this is a finding.

Fix Text: Develop a documented process to notify appropriate personnel when accounts are deleted.

CCI: CCI-001685

Group ID (Vulid): V-224016
Group Title: SRG-OS-000277-GPOS-00107
Rule ID: SV-224016r877856_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000200
Rule Title: The IBM z/OS System Administrator must develop a process to notify appropriate personnel when accounts are removed.
Legacy ID: SV-107845
Legacy ID: V-98741

Vulnerability Discussion: When operating system accounts are disabled, user accessibility is affected. Accounts are utilized for identifying individual operating system users or for identifying the operating system processes themselves. Sending notification of account disabling events to the system administrator and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that operating system accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Check Content:
Ask the system Administrator for the documented process to notify appropriate personnel when accounts are removed.

If there is no documented process, this is a finding.

Fix Text: Develop a documented process to notify appropriate personnel when accounts are removed.

CCI: CCI-001686

Group ID (Vulid): V-224017

Group Title: SRG-OS-000368-GPOS-00154
Rule ID: SV-224017r877857_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-OS-000210
Rule Title: Unsupported IBM z/OS system software must not be installed and/or active on the system.
Legacy ID: SV-107847
Legacy ID: V-98743

Vulnerability Discussion: Control of program execution is a mechanism used to prevent execution of unauthorized programs. Some operating systems may provide a capability that runs counter to the mission or provides users with functionality that exceeds mission requirements. This includes functions and services installed at the operating system level.

Some of the programs, installed by default, may be harmful or may not be necessary to support essential organizational operations (e.g., key missions, functions). Removal of executable programs is not always possible; therefore, establishing a method of preventing program execution is critical to maintaining a secure system baseline.

Methods for complying with this requirement include restricting execution of programs in certain environments, while preventing execution in other environments; or limiting execution of certain program functionality based on organization-defined criteria (e.g., privileges, subnets, sandboxed environments, or roles).

Check Content:
This check applies to all products that meet the following criteria:

- Uses authorized and restricted z/OS interfaces by utilizing Authorized Program Facility (APF) authorized modules or libraries.
- Requires access to system data sets or sensitive information or requires special or privileged authority to run.

For the products in the above category, refer to the vendor's support lifecycle information for current versions and releases.

If the software products currently running on the reviewed system are at a version greater than or equal to the products listed in the vendor's Support Lifecycle information, this is not a finding.

Fix Text: For all products that meet the following criteria:

- Uses authorized and restricted z/OS interfaces by utilizing Authorized Program Facility (APF) authorized modules or libraries.
- Requires access to system data sets or sensitive information or requires special or privileged authority to run.

The ISSO will ensure that unsupported system software for the products in the above category is removed or upgraded prior to a vendor dropping support.

Authorized software that is NO longer supported is a CAT I vulnerability. The customer and site will be given six months to mitigate the risk, develop a supported solution, or obtain a formal letter approving such risk/software.

CCI: CCI-001764

Group ID (Vulid): V-224018
Group Title: SRG-OS-000368-GPOS-00154
Rule ID: SV-224018r877858_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000220
Rule Title: IBM z/OS must not allow nonexistent or inaccessible Link Pack Area (LPA) libraries.
Legacy ID: SV-107849
Legacy ID: V-98745

Vulnerability Discussion: Control of program execution is a mechanism used to prevent execution of unauthorized programs. Some operating systems may provide a capability that runs counter to the mission or provides users with functionality that exceeds mission requirements. This includes functions and services installed at the operating system level.

Some of the programs, installed by default, may be harmful or may not be necessary to support essential organizational operations (e.g., key missions, functions). Removal of executable programs is not always possible; therefore, establishing a method of preventing program execution is critical to maintaining a secure system baseline.

Methods for complying with this requirement include restricting execution of programs in certain environments, while preventing execution in other environments; or limiting execution of certain program functionality based on organization-defined criteria (e.g., privileges, subnets, sandboxed environments, or roles).

Check Content:
From an ISPF Command line enter:
TSO ISRDDN LPA

Review the list.

If there are any DUMMY entries, i.e., inaccessible LPA libraries, this is a finding.

Fix Text: Review all entries contained in the LPA members for the actual existence of each library. Develop a plan of action to correct deficiencies.

The system Link Pack Area (LPA) is the component of MVS that maintains core operating system functions resident in main storage. A security concern exists when libraries from which LPA modules are obtained require APF authorization.

Control over residence in the LPA is specified within the operating system in the following members of the data set SYS1.PARMLIB:

- LPALSTxx specifies the names of libraries to be concatenated to SYS1.LPALIB when the LPA is generated at IPL in an MVS/XA or MVS/ESA system. (The xx is the suffix designated by the LPA parameter in the IEASYSxx member of SYS1.PARMLIB or overridden by the computer operator at system initial program load [IPL].)

- IEAFIXxx specifies the names of modules from SYS1.SVCLIB, the LPALSTxx concatenation, and the LNKLSTxx concatenation that are to be temporarily fixed in central storage in the Fixed LPA (FLPA) for the duration of an IPL. (The xx is the suffix designated by the FIX parameter in the IEASYSxx member of SYS1.PARMLIB or overridden by the computer operator at IPL.)

- IEALPAxx specifies the names of modules that will be loaded from the following:

? SYS1.SVCLIB
? The LPALSTxx concatenation
? The LNKLSTxx concatenation as a temporary extension to the existing Pageable

LPA (PLPA) in the Modified LPA (MLPA) for the duration of an IPL. (The xx is the suffix designated by the MLPA parameter in the IEASYSxx member of SYS1.PARMLIB or overridden by the computer operator at IPL.)

Use the following recommendations and techniques to control the exposures created by the LPA facility:

-The LPALSTxx, IEAFIXxx, and IEALPAxx members will contain only required libraries. On a semiannual basis, Software Support should review the volume serial numbers and verify them in accordance with the system catalog. Software Support will remove all non-existent libraries. The ISSO should modify and/or delete the rules associated with these libraries.

CCI: CCI-001764

Group ID (Vulid): V-224019
Group Title: SRG-OS-000368-GPOS-00154
Rule ID: SV-224019r877859_rule

Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000225
Rule Title: IBM z/OS must not allow nonexistent or inaccessible LINKLIST libraries.
Legacy ID: SV-109619
Legacy ID: V-100515

Vulnerability Discussion: Control of program execution is a mechanism used to prevent execution of unauthorized programs. Some operating systems may provide a capability that runs counter to the mission or provides users with functionality that exceeds mission requirements. This includes functions and services installed at the operating system level.

Some of the programs, installed by default, may be harmful or may not be necessary to support essential organizational operations (e.g., key missions, functions). Removal of executable programs is not always possible; therefore, establishing a method of preventing program execution is critical to maintaining a secure system baseline.

Methods for complying with this requirement include restricting execution of programs in certain environments, while preventing execution in other environments; or limiting execution of certain program functionality based on organization-defined criteria (e.g., privileges, subnets, sandboxed environments, or roles).

Check Content:
From and ISPF Command line enter:
TSO ISRDDN LINKLIST

Review the list, if there are any DUMMY entries i.e., inaccessible LINKLIST libraries, this is a finding.

Fix Text: Review all entries contained in the LINKLIST for the actual existence of each library. Develop a plan of action to correct deficiencies.

The Linklist is a default set of libraries that MVS searches for a specified program. This facility is used so that a user does not have to know the library names in which utility types of programs are stored. Control over membership in the Linklist is specified within the operating system. The data set SYS1.PARMLIB(LNKLSTxx) is used to specify the library names. (The xx is the suffix designated by the LNK parameter in the IEASYSxx member of SYS1.PARMLIB, or overridden by the computer operator at IPL.)

Use the following recommendations and techniques to control the exposures created by the LINKLIST facility:

441-1Avoid inclusion of sensitive libraries in the LNKLSTxx member unless absolutely required.

-The LNKLSTxx and PROGxx (LNKLST entries) members will contain only required libraries. On a semiannual basis, Software Support should review the volume serial numbers, and should verify them in accordance with the system catalog. Software Support will remove all nonexistent libraries. The ISSO should modify and/or delete the rules associated with these libraries.

CCI: CCI-001764

Group ID (Vulid): V-224020
Group Title: SRG-OS-000364-GPOS-00151
Rule ID: SV-224020r877860_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-OS-000230
Rule Title: CA-TSS must be installed and properly configured.
Legacy ID: SV-107851
Legacy ID: V-98747

Vulnerability Discussion: Failure to provide logical access restrictions associated with changes to system configuration may have significant effects on the overall security of the system.

When dealing with access restrictions pertaining to change control, it should be noted that any changes to the hardware, software, and/or firmware components of the operating system can have significant effects on the overall security of the system.

Accordingly, only qualified and authorized individuals should be allowed to obtain access to operating system components for the purposes of initiating changes, including upgrades and modifications.

Logical access restrictions include, for example, controls that restrict access to workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover).

Check Content:
Refer to the active tasks on the system. Use IBM SDSF or the system Log.

If CA-TSS is active this is not a finding.

Fix Text: Ensure that CA-TSS is active on the system.

CCI: CCI-001813

Group ID (Vulid): V-224021
Group Title: SRG-OS-000341-GPOS-00132
Rule ID: SV-224021r877861_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000240
Rule Title: IBM z/OS SMF collection files (system MANx data sets or LOGSTREAM DASD) must have storage capacity to store at least one weeks worth of audit data.
Legacy ID: SV-107853
Legacy ID: V-98749

Vulnerability Discussion: In order to ensure operating systems have a sufficient storage capacity in which to write the audit logs, operating systems need to be able to allocate audit record storage capacity.

The task of allocating audit record storage capacity is usually performed during initial installation of the operating system.

Check Content:
Review the SMF dump procedure in there system.

If the output data sets in the procedure have storage capacity to store at least one weeks' worth of audit data, this is not a finding.

Fix Text: The system Link Pack Area (LPA) is the component of MVS that maintains core operating system functions resident in main storage. A security concern exists when libraries from which LPA modules are obtained require APF authorization.

CCI: CCI-001849

Group ID (Vulid): V-224022
Group Title: SRG-OS-000342-GPOS-00133
Rule ID: SV-224022r877862_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000250
Rule Title: IBM z/OS System Administrators must develop an automated process to collect and retain SMF data.
Legacy ID: SV-107855
Legacy ID: V-98751

Vulnerability Discussion: Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Check Content:
Ask the system administrator if there is an automated process is in place to collect and retain all SMF data produced on the system.

If, based on the information provided, it can be determined that an automated process is in place to collect and retain all SMF data produced on the system, this is not a finding.

If it cannot be determined this process exists and is being adhered to, this is a finding.

Fix Text: Ensure that an automated process is in place to collect SMF data.

Review SMF data collection and retention processes. Develop processes that are automatically started to dump SMF collection files immediately upon their becoming full.

To ensure that all SMF data is collected in a timely manner, and to reduce the risk of data loss, ensure that automated mechanisms are in place to collect and retain all SMF data produced on the system. Dump the SMF files (MANx) in systems based on the following guidelines:

-Dump each SMF file as it fills up during the normal course of daily processing.
-Dump all remaining SMF data at the end of each processing day.

Establish a process using Audit logging.

CCI: CCI-001851

Group ID (Vulid): V-224023
Group Title: SRG-OS-000355-GPOS-00143
Rule ID: SV-224023r877863_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000270
Rule Title: The IBM z/OS SNTP daemon (SNTPD) must be active.
Legacy ID: V-98755
Legacy ID: SV-107859

Vulnerability Discussion: Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a

system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Check Content:
From UNIX System Services ISPF Shell, navigate to ribbon select tools.
Select option 1 - Work with Processes.

If SNTP Daemon (SNTPD) is not active, this is a finding.

Fix Text: Obtain a copy of this sample procedure from SEZAINST and store it in one of your PROCLIB concatenation data sets.

Perform the following step to start SNTPD as a procedure:
Invoke the procedure using the system operator start command. The following sample, SEZAINST(SNTPD), shows how to start SNTPD as a procedure:

```
//*
//* Sample procedure for the Simple Network Time Protocol (SNTP)
//*
//* z/OS Communications Server Version 1 Release 13
//* SMP/E Distribution Name: SEZAINST(EZASNPRO)
//*
//* Copyright: Licensed Materials - Property of IBM
//* 5650-ZOS
//* Copyright IBM Corp. 2002, 2015
//*
//* Status: CSV2R2
//*
//SNTPD EXEC PGM=SNTPD,REGION=4096K,TIME=NOLIMIT,
// PARM='/ -d'
//SYSPRINT DD SYSOUT=*,DCB=(RECFM=F,LRECL=132,BLKSIZE=132)
//SYSIN DD DUMMY
//SYSERR DD SYSOUT=*
//SYSOUT DD SYSOUT=*,DCB=(RECFM=F,LRECL=132,BLKSIZE=132)
//CEEDUMP DD SYSOUT=*
//SYSABEND DD SYSOUT=*
```

CCI: CCI-001891

Group ID (Vulid): V-224024
Group Title: SRG-OS-000355-GPOS-00143
Rule ID: SV-224024r877864_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000280
Rule Title: IBM z/OS SNTP daemon (SNTPD) permission bits must be properly configured.
Legacy ID: V-98757
Legacy ID: SV-107861

Vulnerability Discussion: Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Check Content:
From the ISPF Command Shell enter:
cd /usr/sbin
ls -al

If the following File permission and user Audit Bits are true, this is not a finding.

/usr/sbin/sntpd 1740 faf

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
- no auditing

Fix Text: With the assistance of a systems programmer with UID(0) and/or SUPERUSER access, configure the UNIX permission bits and user audit bits on the SNTPD to conform to the specifications below:

/usr/sbin/sntpd 1740 faf

CCI: CCI-001891

Group ID (Vulid): V-224025
Group Title: SRG-OS-000356-GPOS-00144
Rule ID: SV-224025r877865_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000290
Rule Title: IBM z/OS PARMLIB CLOCKxx must have the Accuracy PARM coded properly.
Legacy ID: V-98759
Legacy ID: SV-107863

Vulnerability Discussion: Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network. Organizations should consider setting time periods for different types of systems (e.g., financial, legal, or mission-critical systems).

Organizations should also consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints). This requirement is related to the comparison done every 24 hours in SRG-OS-000355 because a comparison must be done in order to determine the time difference.

Check Content:
Refer to the CLOCKxx member of PARMLIB.

If the ACCURACY parm is not coded, this is a finding.

If the ACCURACY parm is coded to "1000", this is not a finding.

Fix Text: Define the CLOCKxx statement to include the ACCURACY parm set to "1000".

CCI: CCI-002046

Group ID (Vulid): V-224026
Group Title: SRG-OS-000420-GPOS-00186
Rule ID: SV-224026r877866_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000300
Rule Title: The IBM z/OS Policy Agent must contain a policy that protects against or limits the effects of denial-of-service (DoS) attacks by ensuring IBM z/OS is implementing rate-limiting measures on impacted network interfaces.
Legacy ID: V-98761
Legacy ID: SV-107865

Vulnerability Discussion: DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of the operating system to mitigate the impact of DoS attacks that have occurred or are ongoing on system availability. For each system, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or establishing memory partitions). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

Check Content:
Examine the "Policy Agent" policy statements.

If it can be determined that the policy that protects against or limits the effects of denial-of-service (DoS) attacks by ensuring the operating system is implementing rate-limiting measures on impacted network interfaces, this is not a finding.

Fix Text: Develop "Policy Agent" statements to protect against or limit the effects of denial-of-service (DoS) attacks by ensuring the operating system is implementing rate-limiting measures on impacted network interfaces.

CCI: CCI-002385

Group ID (Vulid): V-251108

Group Title: SRG-OS-000404-GPOS-00183
Rule ID: SV-251108r877949_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000320
Rule Title: The IBM z/OS systems requiring data at rest protection must properly employ IBM DS8880 or equivalent hardware solutions for full disk encryption.
Legacy ID: V-98765
Legacy ID: SV-107869

Vulnerability Discussion: This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. Operating systems handling data requiring "data at rest" protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.

Selection of a cryptographic mechanism is based on the need to protect the integrity of organizational information. The strength of the mechanism is commensurate with the security category and/or classification of the information. Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).

Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Satisfies: SRG-OS-000185-GPOS-00079, SRG-OS-000405-GPOS-00184, SRG-OS-000404-GPOS-00183, SRG-OS-000396-GPOS-00176

Check Content:
Determine if IBM's DS880 Disks or equivalent hardware solutions are in use.

If IBMs DS880 Disks or equivalent hardware solutions are not in use for systems that require "data at rest", this is a finding.

Fix Text: Employ IBM's DS8880 hardware or equivalent hardware solutions to ensure full disk encryption.

CCI: CCI-002476

CCI: CCI-001199

CCI: CCI-002420

CCI: CCI-002445

CCI: CCI-002446

Group ID (Vulid): V-224029
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-224029r877867_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000330
Rule Title: IBM z/OS must employ a session manager to manage retaining a users session lock until that user reestablishes access using established identification and authentication procedures.
Legacy ID: SV-107871
Legacy ID: V-98767

Vulnerability Discussion: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

Regardless of where the session lock is determined and implemented, once invoked, the session lock will remain in place until the user re-authenticates. No other activity aside from re-authentication will unlock the system.

Check Content:
Verify the any Session Manager in use retains a user's session lock until that user reestablishes access using established identification and authentication procedures.

If it does not, this is a finding.

Fix Text: Configure any Session Manager in use to retain a user's session lock until that user reestablishes access using established identification and authentication procedures.

CCI: CCI-000366

Group ID (Vulid): V-224031
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-224031r877869_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000350
Rule Title: IBM z/OS must configure system wait times to protect resource availability based on site priorities.
Legacy ID: SV-107875
Legacy ID: V-98771

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Check Content:
Refer to IEASYS00 member in SYS1.PARMLIB Concatenation. Determine proper SMFPRMxx member.

Examine the JWT, SWT, and TWT values.

If the JWT parameter is greater than "15" minutes, and the system is processing unclassified information, review the following items.

If any of these items is true, this is not a finding.

-If a session is not terminated, but instead is locked out after 15 minutes of inactivity, a process must be in place that requires user identification and authentication before the session is unlocked. Session lock-out will be implemented through system controls or terminal screen protections.

-A system's default time for terminal lock-out or session termination may be lengthened to 30 minutes at the discretion of the ISSM or ISSO. The ISSM and/or ISSO will maintain the documentation for each system with a time-out adjusted beyond the 15-minute recommendation

to explain the basis for this decision.

-The ISSM and/or ISSO may set selected userids to have a time-out of up to 60 minutes in order to complete critical reports or transactions without timing out. Each exception must meet the following criteria:
-The time-out exception cannot exceed 60 minutes.
-A letter of justification fully documenting the user requirement(s) must be submitted and approved by the site ISSM or ISSO. In addition, this letter must identify an alternate means of access control for the terminal(s) involved (e.g., a room that is locked at all times, a room with a cipher lock to limit access, a password protected screen saver set to 30 minutes or less, etc.).
-The requirement must be revalidated on an annual basis.

If the TWT and SWT values are equal or less than the JWT value, this is not a finding.

Fix Text: Configure the SMFPRMxx JWT to "15" minutes for classified systems.

The JWT parameter can be greater than "15" minutes if the system is processing unclassified information and the following items are reviewed.

-If a session is not terminated, but instead is locked out after "15" minutes of inactivity, a process must be in place that requires user identification and authentication before the session is unlocked. Session lock-out will be implemented through system controls or terminal screen protections.

-A system's default time for terminal lock-out or session termination may be lengthened to "30" minutes at the discretion of the ISSM or ISSO. The ISSM and/or ISSO will maintain the documentation for each system with a time-out adjusted beyond the 15-minute recommendation to explain the basis for this decision.

-The ISSM and/or ISSO may set selected userids to have a time-out of up to "60" minutes in order to complete critical reports or transactions without timing out. Each exception must meet the following criteria:

-The time-out exception cannot exceed "60" minutes.

-A letter of justification fully documenting the user requirement(s) must be submitted and approved by the site ISSM or ISSO. In addition, this letter must identify an alternate means of access control for the terminal(s) involved (e.g., a room that is locked at all times, a room with a cipher lock to limit access, a password protected screen saver set to 30 minutes or less, etc.).

-The requirement must be revalidated on an annual basis.

Configure any TWT and or SWT to be equal or less than the JWT.

CCI: CCI-000366

Group ID (Vulid): V-224032
Group Title: SRG-OS-000031-GPOS-00012
Rule ID: SV-224032r877870_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000360
Rule Title: IBM z/OS must employ a session manager to conceal, via the session lock, information previously visible on the display with a publicly viewable image.
Legacy ID: SV-107877
Legacy ID: V-98773

Vulnerability Discussion: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. The operating system session lock event must include an obfuscation of the display screen so as to prevent other users from reading what was previously displayed.

Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, a clock, a battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.

Check Content:
Ask the system administrator for the configuration parameters for the session manager in use.

If there is no session manager in use, this is a finding.

If the session manager is not configured to conceal, via the session lock, information previously visible on the display with a publicly viewable image, this is a finding.

Fix Text: Configure the session manager to conceal, via the session lock, information previously visible on the display with a publicly viewable image.

CCI: CCI-000060

Group ID (Vulid): V-224033
Group Title: SRG-OS-000029-GPOS-00010
Rule ID: SV-224033r877871_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000370

Rule Title: IBM z/OS must employ a session manager to initiate a session lock after a 15-minute period of inactivity for all connection types.
Legacy ID: SV-107879
Legacy ID: V-98775

Vulnerability Discussion: A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Check Content:
Ask the system administrator for the configuration parameters for the session manager in use.

If there is no session manager in use, this is a finding.

If the session manager is not configured to initiate a session lock after a 15-minute period of inactivity, this is a finding.

Fix Text: Configure the session manager to initiate a session lock after a 15-minute period of inactivity.

CCI: CCI-000057

Group ID (Vulid): V-224034
Group Title: SRG-OS-000028-GPOS-00009
Rule ID: SV-224034r877872_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000380
Rule Title: IBM z/OS must employ a session manager to manage retaining a users session lock until that user reestablishes access using established identification and authentication procedures.
Legacy ID: V-98777
Legacy ID: SV-107881

Vulnerability Discussion: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

Regardless of where the session lock is determined and implemented, once invoked, the session lock must remain in place until the user re-authenticates. No other activity aside from re-authentication will unlock the system.

Check Content:
Ask the system administrator for the configuration parameters for the session manager in use.

If there is no session manager in use, this is a finding.

If the session manager is not configured to retain a user's session lock until that user reestablishes access using established identification and authentication procedures, this is a finding.

Fix Text: LPA (PLPA) in the Modified LPA (MLPA) for the duration of an IPL. (The xx is the suffix designated by the MLPA parameter in the IEASYSxx member of SYS1.PARMLIB or overridden by the computer operator at IPL.)

CCI: CCI-000056

Group ID (Vulid): V-224035
Group Title: SRG-OS-000002-GPOS-00002
Rule ID: SV-224035r877873_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000390
Rule Title: IBM z/OS system administrator must develop a procedure to remove or disable temporary user accounts after 72 hours.
Legacy ID: SV-107883
Legacy ID: V-98779

Vulnerability Discussion: If temporary user accounts remain active when no longer needed or for an excessive period, these accounts may be used to gain unauthorized access. To mitigate this risk, automated termination of all temporary accounts must be set upon account creation.

Temporary accounts are established as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation.

If temporary accounts are used, the operating system must be configured to automatically terminate these types of accounts after a DoD-defined time period of 72 hours.

To address access requirements, many operating systems may be integrated with enterprise-level

authentication/access mechanisms that meet or exceed access control policy requirements.

Check Content:
Ask the system administrator for the procedure to automatically remove or disable temporary user accounts after 72 hours.

If there is no procedure, this is a finding.

Fix Text: Develop a procedure to remove or disable emergency user accounts after the crisis is resolved or 72 hours.

CCI: CCI-000016

Group ID (Vulid): V-224036
Group Title: SRG-OS-000123-GPOS-00064
Rule ID: SV-224036r877874_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000400
Rule Title: IBM z/OS system administrator must develop a procedure to remove or disable emergency accounts after the crisis is resolved or 72 hours.
Legacy ID: V-102937
Legacy ID: SV-111899

Vulnerability Discussion: Emergency accounts are privileged accounts that are established in response to crisis situations where the need for rapid account activation is required. Therefore, emergency account activation may bypass normal account authorization processes. If these accounts are automatically disabled, system maintenance during emergencies may not be possible, thus adversely affecting system availability.

Emergency accounts are different from infrequently used accounts (i.e., local logon accounts used by the organization's system administrators when network or normal logon/access is not available). Infrequently used accounts are not subject to automatic termination dates. Emergency accounts are accounts created in response to crisis situations, usually for use by maintenance personnel. The automatic expiration or disabling time period may be extended as needed until the crisis is resolved; however, it must not be extended indefinitely. A permanent account should be established for privileged users who need long-term maintenance accounts.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

Check Content:

Ask the system administrator for the procedure to automatically remove or disable emergency accounts after the crisis is resolved or 72 hours.

If there is no procedure, this is a finding.

Fix Text: Develop a procedure to remove or disable emergency user accounts after the crisis is resolved or 72 hours.

CCI: CCI-001682

Group ID (Vulid): V-224037
Group Title: SRG-OS-000304-GPOS-00121
Rule ID: SV-224037r877875_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000410
Rule Title: IBM z/OS system administrator must develop a procedure to notify System Administrators and ISSOs of account enabling actions.
Legacy ID: SV-107885
Legacy ID: V-98781

Vulnerability Discussion: Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to enable an existing disabled account. Sending notification of account enabling actions to the System Administrator and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that operating system accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

In order to detect and respond to events that affect user accessibility and application processing, operating systems must audit account enabling actions and, as required, notify the appropriate individuals so they can investigate the event.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Check Content:
Ask the system administrator for the procedure to notify system administrators and ISSOs of account enabling actions. If there is no procedure, this is a finding.

Fix Text: Develop a documented procedure to notify system administrators and ISSOs of account enabling actions.

CCI: CCI-002132

Group ID (Vulid): V-224038
Group Title: SRG-OS-000363-GPOS-00150
Rule ID: SV-224038r877876_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000420
Rule Title: IBM z/OS system administrator must develop a procedure to notify designated personnel if baseline configurations are changed in an unauthorized manner.
Legacy ID: SV-107887
Legacy ID: V-98783

Vulnerability Discussion: Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating system's IMO/ISSO and SAs must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Check Content:
Ask the system administrator for the procedure to notify designated personnel if baseline configurations are changed in an unauthorized manner.

If there is no procedure, this is a finding.

Fix Text: Develop a procedure to notify designated personnel if baseline configurations are changed in an unauthorized manner.

CCI: CCI-001744

Group ID (Vulid): V-224039
Group Title: SRG-OS-000126-GPOS-00066
Rule ID: SV-224039r877877_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000440
Rule Title: IBM z/OS system administrator must develop a procedure to terminate all sessions

and network connections related to nonlocal maintenance when nonlocal maintenance is completed.
Legacy ID: SV-107889
Legacy ID: V-98785

Vulnerability Discussion: If a maintenance session or connection remains open after maintenance is completed, it may be hijacked by an attacker and used to compromise or damage the system.

Some maintenance and test tools are either standalone devices with their own operating systems or are applications bundled with an operating system.

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

Check Content:
Ask the system administrator for the procedure to terminate all sessions and network connections related to nonlocal maintenance when nonlocal maintenance is completed.

If there is no procedure, this is a finding.

Fix Text: Develop a procedure to terminate all sessions and network connections related to nonlocal maintenance when nonlocal maintenance is completed.

CCI: CCI-000879

Group ID (Vulid): V-224040
Group Title: SRG-OS-000437-GPOS-00194
Rule ID: SV-224040r877878_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000450
Rule Title: IBM z/OS system administrator must develop a procedure to remove all software components after updated versions have been installed.
Legacy ID: SV-107891
Legacy ID: V-98787

Vulnerability Discussion: Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some

information technology products may remove older versions of software automatically from the information system.

Check Content:
Ask the system administrator for the procedure to remove all software components after updated versions have been installed.

If there is no procedure, this is a finding.

Fix Text: Develop a procedure to remove all software components after updated versions have been installed.

CCI: CCI-002617

Group ID (Vulid): V-224041
Group Title: SRG-OS-000447-GPOS-00201
Rule ID: SV-224041r877879_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000460
Rule Title: IBM z/OS system administrator must develop a procedure to shut down the information system, restart the information system, and/or notify the system administrator when anomalies in the operation of any security functions are discovered.
Legacy ID: SV-107893
Legacy ID: V-98789

Vulnerability Discussion: If anomalies are not acted upon, security functions may fail to secure the system.

Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

Notifications provided by information systems include messages to local computer consoles, and/or hardware indications, such as lights.

This capability must take into account operational requirements for availability for selecting an appropriate response. The organization may choose to shut down or restart the information system upon security function anomaly detection.

Check Content:
Ask the system administrator for the procedure to shut down the information system, restart the information system, and/or notify the system administrator when anomalies occur.

If a procedure does not exist, this is a finding.

If the procedure does not properly shut down the information system, restart the information system, and/or notify the system administrator when anomalies occur, this is a finding.

Fix Text: Develop a procedure to shut down the information system, restart the information system, and/or notify the system administrator when anomalies occur.

CCI: CCI-002702

Group ID (Vulid): V-224042
Group Title: SRG-OS-000479-GPOS-00224
Rule ID: SV-224042r877880_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000470
Rule Title: IBM z/OS system administrator must develop a procedure to offload SMF files to a different system or media than the system being audited.
Legacy ID: SV-107895
Legacy ID: V-98791

Vulnerability Discussion: The task of allocating audit record storage capacity is usually performed during initial installation of the operating system.

Check Content:
Ask the system administrator for the procedure to offload SMF files to a different system or media than the system being audited.

If the procedure does not exist, this is a finding.

Fix Text: Develop a procedure to offload SMF files to a different system or media than the system being audited.

CCI: CCI-001851

Group ID (Vulid): V-224043
Group Title: SRG-OS-000030-GPOS-00011

Rule ID: SV-224043r877881_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-OS-000480
Rule Title: IBM z/OS must employ a session manager for users to directly initiate a session lock for all connection types.
Legacy ID: SV-107897
Legacy ID: V-98793

Vulnerability Discussion: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, operating systems need to provide users with the ability to manually invoke a session lock so users may secure their session should the need arise for them to temporarily vacate the immediate physical vicinity.

Check Content:
Ask the system administrator for the configuration parameters for the session manager in use.

If there is no session manager in use this is a finding.

If the session manager in use does not allow users to directly initiate a session lock for all connection types, this is a finding.

Fix Text: Configure the session manager to allow users to directly initiate a session lock for all connection types.

CCI: CCI-000058

Group ID (Vulid): V-224044
Group Title: SRG-OS-000033-GPOS-00014
Rule ID: SV-224044r877882_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-SH-000020
Rule Title: The SSH daemon must be configured to use a FIPS 140-2 compliant cryptographic algorithm.
Legacy ID: V-98795
Legacy ID: SV-107899

Vulnerability Discussion: Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000120-GPOS-00061, SRG-OS-000250-GPOS-00093

Check Content:
Locate the SSH daemon configuration file which may be found in /etc/ssh/ directory.

Alternately:
From UNIX System Services ISPF Shell navigate to ribbon select tools.
Select option 1 - Work with Processes.

If SSH Daemon is not active, this is not a finding.

Examine SSH daemon configuration file.
sshd_config

If there are no Ciphers lines or the ciphers list contains any cipher not starting with "3des" or "aes", this is a finding.

If the MACs line is not configured to "hmac-sha1" or greater, this is a finding.

Examine the z/OS-specific sshd server system-wide configuration:
zos_sshd_config

If any of the following is untrue, this is a finding.

FIPSMODE=YES
CiphersSource=ICSF
MACsSource=ICSF

Fix Text: Edit the SSH daemon configuration and remove any ciphers not starting with "3des" or "aes". If necessary, add a "Ciphers" line using FIPS 140-2 compliant algorithms.

CCI: CCI-000068

CCI: CCI-000803

CCI: CCI-001453

Group ID (Vulid): V-224045
Group Title: SRG-OS-000096-GPOS-00050
Rule ID: SV-224045r877883_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-SH-000030
Rule Title: IBM z/OS SSH daemon must be configured to only use the SSHv2 protocol.
Legacy ID: V-98797
Legacy ID: SV-107901

Vulnerability Discussion: In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., VPN and IPS); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the operating system must support the organizational requirements, providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

Check Content:
Locate the SSH daemon configuration file.
May be found in /etc/ssh/ directory.

Alternately:
From UNIX System Services ISPF Shell navigate to ribbon select tools.
Select option 1 - Work with Processes.

If SSH Daemon is not active, this is not a finding.

Examine SSH daemon configuration file.

If the variables "Protocol 2,1" or "Protocol 1" are defined on a line without a leading comment, this is a finding.

Fix Text: Edit the sshd_config file and set the "Protocol" setting to "2".

CCI: CCI-000382

Group ID (Vulid): V-224046
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224046r877884_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-SL-000010
Rule Title: IBM z/OS permission bits and user audit bits for HFS objects that are part of the Syslog daemon component must be configured properly.
Legacy ID: V-98799
Legacy ID: SV-107903

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
From an ISPF
Enter
cd /usr/sbin
Enter
ls -alW
If File Permission Bits and User Audit Bits for SYSLOG Daemon HFS directories and files are as below this is not a finding.
/usr/sbin/syslogd 1740 fff

Enter
cd /etc/
Enter

ls -alW

If File Permission Bits and User Audit Bits for Output log file defined in the configuration file are as below this is not a finding.
/etc/syslog.conf 0744 faf
0744 fff

Notes:
The /usr/sbin/syslogd object is a symbolic link to /usr/lpp/tcpip/sbin/syslogd. The permission and user audit bits on the target of the symbolic link must have the required settings.
The /etc/syslog.conf file may not be the configuration file the daemon uses. It is necessary to check the script or JCL used to start the daemon to determine the actual configuration file. For example, in /etc/rc:
_BPX_JOBNAME='SYSLOGD' /usr/sbin/syslogd -f /etc/syslog.conf

For example, in the SYSLOGD started task JCL:

//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT
// PARM='POSIX(ON) ALL31(ON)/ -f /etc/syslogd.conf'

//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT
// PARM='POSIX(ON) ALL31(ON) /-f //"SYS1.TCPPARMS(SYSLOG)"'

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
- no auditing

Fix Text: Configure the UNIX permission bits and user audit bits on the HFS directories and files for the Syslog daemon to conform to the specifications in the SYSLOG Daemon HFS Object Security Settings table below.

Log files should have security that prevents anyone except the syslogd process and authorized maintenance jobs from writing to or deleting them.

A maintenance process to periodically clear the log files is essential. Logging stops if the target file system becomes full.

SYSLOG Daemon HFS Object Security Settings
File Permission Bits User Audit Bits
/usr/sbin/syslogd 1740 fff
[Configuration File]
/etc/syslog.conf 0744 faf
[Output log file defined in the configuration file]
0744 fff

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
- no auditing

NOTES:
The /usr/sbin/syslogd object is a symbolic link to /usr/lpp/tcpip/sbin/syslogd. The permission and user audit bits on the target of the symbolic link must have the required settings.

The /etc/syslog.conf file may not be the configuration file the daemon uses. It is necessary to check the script or JCL used to start the daemon to determine the actual configuration file. For example, in /etc/rc:

_BPX_JOBNAME='SYSLOGD' /usr/sbin/syslogd -f /etc/syslog.conf

For example, in the SYSLOGD started task JCL:

//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT
// PARM='POSIX(ON) ALL31(ON)/ -f /etc/syslogd.conf'

//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT
// PARM='POSIX(ON) ALL31(ON) /-f //"SYS1.TCPPARMS(SYSLOG)"'

The following commands can be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

chmod 1740 /usr/lpp/tcpip/sbin/syslogd
chaudit rwx=f /usr/lpp/tcpip/sbin/syslogd
chmod 0744 /etc/syslog.conf
chaudit w=sf,rx+f /etc/syslog.conf
chmod 0744 /log_dir/log_file
chaudit rwx=f /log_dir/log_file

CCI: CCI-000213

Group ID (Vulid): V-224047
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-224047r877885_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-SL-000020
Rule Title: The IBM z/OS Syslog daemon must not be started at z/OS initialization.
Legacy ID: V-98801
Legacy ID: SV-107905

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
SYSLOGD may be started from the shell, a cataloged procedure (STC), or the BPXBATCH program. Additionally, other mechanisms (e.g., a job scheduler) may be used to automatically

start the Syslog daemon. To thoroughly analyze this requirement you may need to view the OS SYSLOG using SDSF, find the last IPL, and look for the initialization of SYSLOGD.

If the Syslog daemon SYSLOGD is started automatically during the initialization of the z/S/ system, this is not a finding.

Fix Text: Review the files used to initialize tasks during system IPL (e.g., /etc/rc, SYS1.PARMLIB, any job scheduler definitions) configure the Syslog daemon to start automatically during z/OS system initialization.

It is important that syslogd be started during the initialization phase of the z/OS system to ensure that significant messages are not lost. As with other z/OS UNIX daemons, there is more than one way to start SYSLOGD. It can be started as a process in the /etc/rc file or as a z/OS started task.

CCI: CCI-000764

Group ID (Vulid): V-224048
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-224048r877886_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-SL-000030
Rule Title: The IBM z/OS Syslog daemon must be properly defined and secured.
Legacy ID: V-98803
Legacy ID: SV-107907

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
From the ISPF Command Shell enter:
TSS LIST(SYSLOGD) SEGMENT(OMVS)

If the following guidance is true, this is not a finding.

-The Syslog daemon userid is SYSLOGD.
-The SYSLOGD userid has the STC facility.
-The SYSLOGD userid has UID(0), HOME('/'), and PROGRAM('/bin/sh') specified in the OMVS segment.
-The SYSLOGD started proc is assigned the SYSLOGD userid is in the Started Task Table.

If Syslog daemon is started from /etc/rc then from the ISPF Command Shell enter:
OMVS
cd /etc
cat rc

If Syslog daemon is started from /etc/rc then ensure that the "_BPX_JOBNAME" and "_BPX_USERID" environment variables are assigned a value of SYSLOGD.

If the Syslog daemon is started from /etc/rc and the "_BPX_JOBNAME" and "_BPX_USERID" environment variables are not assigned a value of SYSLOGD, this is a finding.

Fix Text: Configure so that the Syslog daemon runs under its own user account. Specifically, it does not share the account defined for the z/OS UNIX kernel.

The Syslog daemon userid is SYSLOGD.
The SYSLOGD userid has the STC facility.
The SYSLOGD userid has UID(0), HOME('/'), and PROGRAM('/bin/sh') specified in the OMVS segment.

To set up and use as an MVS Started Proc, the following sample commands are provided:

TSS CREATE(SYSLOGD) TYPE(USER) NAME(SYSLOGD) -
DEPT(existing-dept) FACILITY(STC) -
PASSWORD(password,0)
TSS ADD(SYSLOGD) DFLTGRP(stctcpx) GROUP(stctcpx)
TSS ADD(SYSLOGD) SOURCE(INTRDR)
TSS ADD(SYSLOGD) UID(0) HOME(/) OMVSPGM(/bin/sh)

The SYSLOGD started proc is assigned the SYSLOGD userid is in the Started Task Table.

TSS ADD(STC) PROCNAME(SYSLOGD) ACID(SYSLOGD)

If /etc/rc is used to start the Syslog daemon, ensure that the _BPX_JOBNAME and _BPX_ USERID environment variables are assigned a value of SYSLOGD.

CCI: CCI-000764

Group ID (Vulid): V-224049
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224049r877887_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-SM-000010
Rule Title: IBM z/OS DFSMS resources must be protected in accordance with the proper security requirements.
Legacy ID: V-98805
Legacy ID: SV-107909

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000324-GPOS-00125

Check Content:
If all SMS resources and/or generic equivalent are properly protected according to the requirements specified and the following guidance is true, this is not a finding.

The TSS resources are owned or DEFPROT is specified for the resource class.

To avoid authorization failures once a base cluster is accessed via a PATH or AIX by a user or application that has authority to the PATH and AIX, but not the base cluster, APAR OA50118 must be applied.

The resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE is defined with access of

NONE.
The resource STGADMIN.IGG.CATALOG.SECURITY.BOTH is defined with access of READ.

Note: The resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE can be defined with read access for migration purposes. If it is, a detailed migration plan must be documented and filed by the ISSM that determines a definite migration period. All access must be logged. At the completion of migration, this resource must be configured with access of NONE.

If the resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE and STGADMIN.IGG.CATALOG.SECURITY.BOTH are both defined, ADMIN.IGG.CATALOG.SECURITY.BOTH takes precedence.

STGADMIN.DPDSRN.olddsname is restricted to system programmers and all access is logged.

The STGADMIN.IGD.ACTIVATE.CONFIGURATION is restricted to system programmers and all access is logged.

The STGADMIN.IGG.DEFDEL.UALIAS is restricted to centralized and decentralized security personnel and system programmers and all access is logged.

The following resources and prefixes may be available to the end user.

STGADMIN.ADR.COPY.CNCURRNT
STGADMIN.ADR.COPY.FLASHCPY
STGADMIN.ADR.COPY.TOLERATE.ENQF
STGADMIN.ADR.DUMP.CNCURRNT
STGADMIN.ADR.DUMP.TOLERATE.ENQF
STGADMIN.ADR.RESTORE.TOLERATE.ENQF
STGADMIN.ARC.ENDUSER.
STGADMIN.IGG.ALTER.SMS

The following resource is restricted to Application Production Support Team members, Automated Operations, DASD managers, and system programmers.

STGADMIN.IDC.DCOLLECT

The following resources are restricted to Application Production Support Team members, DASD managers, and system programmers.

STGADMIN.ARC.CANCEL
STGADMIN.ARC.LIST
STGADMIN.ARC.QUERY
STGADMIN.ARC.REPORT
STGADMIN.DMO.CONFIG
STGADMIN.IFG.READVTOC

STGADMIN.IGG.DELGDG.FORCE

The following resource prefixes, at a minimum, are restricted to DASD managers and system programmers.

STGADMIN.ADR
STGADMIN.ANT
STGADMIN.ARC
STGADMIN.DMO
STGADMIN.ICK
STGADMIN.IDC
STGADMIN.IFG
STGADMIN.IGG
STGADMIN.IGWSHCDS

The following Storage Administrator functions prefix is restricted to DASD managers and system programmers and all access is logged.

STGADMIN.ADR.STGADMIN.

Fix Text: Ensure that the following are properly specified in the ESM.

Note: The resources and/or resource prefixes identified below are examples of a possible installation. The actual resource type, resources, and/or resource prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.

Below is listed the access requirements for SMS Resources. Ensure the guidelines for the resources and/or generic equivalent are followed.

The TSS resources are owned and/or DEFPROT is specified for the resource class.

Configure resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE with no access.
Note: The resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE can be defined with read access for migration purposes. If it is, a detailed migration plan must be documented and filed with the ISSM that determines a definite migration period. All access must be logged. At the completion of migration this resource must be configured with access = NONE.

Configure STGADMIN.IGG.CATALOG.SECURITY.BOTH to have READ access for all.

TSS ADD(ADMIN) IBMFAC(STGADMIN)
or
TSS REPLACE(RDT) RESCLASS(IBMFAC) ATTR(DEFPROT)
The STGADMIN.DPDSRN.olddsname is restricted to System Programmers and all access is logged.

Example:
TSS PERMIT(syspsmpl) IBMFAC(STGADMIN.DPDSRN.olddsname) -
ACCESS(READ) ACTION(AUDIT)

The STGADMIN.IGD.ACTIVATE.CONFIGURATION is restricted to system programmers and all access is logged.

Example:
TSS PERMIT(syspsmpl) IBMFAC(STGADMIN.IGD.ACTIVATE.CONFIGURATION) -
ACCESS(READ) ACTION(AUDIT)

The STGADMIN.IGG.DEFDEL.UALIAS is restricted to system programmers and security personnel and all access is logged.

Example:
TSS PERMIT(secasmpl) IBMFAC(STGADMIN.IGG.DEFDEL.UALIAS) -
ACCESS(READ) ACTION(AUDIT)
TSS PERMIT(secdsmpl) IBMFAC(STGADMIN.IGG.DEFDEL.UALIAS) -
ACCESS(READ) ACTION(AUDIT)
TSS PERMIT(syspsmpl) IBMFAC(STGADMIN.IGG.DEFDEL.UALIAS) -
ACCESS(READ) ACTION(AUDIT)

The following resources and prefixes may be available to the end user.

Example:
STGADMIN.ADR.COPY.CNCURRNT
STGADMIN.ADR.COPY.FLASHCPY
STGADMIN.ADR.COPY.TOLERATE.ENQF
STGADMIN.ADR.DUMP.CNCURRNT
STGADMIN.ADR.DUMP.TOLERATE.ENQF
STGADMIN.ADR.RESTORE.TOLERATE.ENQF
STGADMIN.ARC.ENDUSER.
STGADMIN.IGG.ALTER.SMS

Example:
TSS PERMIT(endusers) IBMFAC(STGADMIN.ADR.COPY.CNCURRNT.) -
ACCESS(READ)

The following resource is restricted to Application Production Support Team members, Automated Operations, DASD managers, and system programmers.

STGADMIN.IDC.DCOLLECT

Example:
TSS PERMIT(appssmpl) IBMFAC(STGADMIN.IDC.DCOLLECT) ACCESS(READ)
TSS PERMIT(autosmpl) IBMFAC(STGADMIN.IDC.DCOLLECT) ACCESS(READ)

TSS PERMIT(dasbsmpl) IBMFAC(STGADMIN.IDC.DCOLLECT) ACCESS(READ)
TSS PERMIT(dasdsmpl) IBMFAC(STGADMIN.IDC.DCOLLECT) ACCESS(READ)
TSS PERMIT(syspsmpl) IBMFAC(STGADMIN.IDC.DCOLLECT) ACCESS(READ)

The following resources are restricted to Application Production Support Team members, DASD managers, and system programmers.

Example:
STGADMIN.ARC.CANCEL
STGADMIN.ARC.LIST
STGADMIN.ARC.QUERY
STGADMIN.ARC.REPORT
STGADMIN.DMO.CONFIG
STGADMIN.IFG.READVTOC
STGADMIN.IGG.DELGDG.FORCE

Example:
TSS PERMIT(appssmpl) IBMFAC(STGADMIN.ARC.CANCEL) ACCESS(READ)
TSS PERMIT(dasbsmpl) IBMFAC(STGADMIN.ARC.CANCEL) ACCESS(READ)
TSS PERMIT(dasdsmpl) IBMFAC(STGADMIN.ARC.CANCEL) ACCESS(READ)
TSS PERMIT(syspsmpl) IBMFAC(STGADMIN.ARC.CANCEL) ACCESS(READ)

The following resource prefixes, at a minimum, are restricted to DASD managers and system programmers.

STGADMIN.ADR
STGADMIN.ANT
STGADMIN.ARC
STGADMIN.DMO
STGADMIN.ICK
STGADMIN.IDC
STGADMIN.IFG
STGADMIN.IGG
STGADMIN.IGWSHCDS

Example:

TSS PERMIT(dasbsmpl) IBMFAC(STGADMIN.ADR) ACCESS(READ)
TSS PERMIT(dasdsmpl) IBMFAC(STGADMIN.ADR) ACCESS(READ)
TSS PERMIT(syspsmpl) IBMFAC(STGADMIN.ADR) ACCESS(READ)

The following Storage Administrator functions prefix is restricted to DASD managers and system programmers and all access is logged.

STGADMIN.ADR.STGADMIN.

Example:

TSS PERMIT(dasbsmpl) IBMFAC(STGADMIN.ADR.STGADMIN.) ACCESS(READ) - ACTION(AUDIT)
TSS PERMIT(dasdsmpl) IBMFAC(STGADMIN.ADR.STGADMIN.) ACCESS(READ) - ACTION(AUDIT)
TSS PERMIT(syspsmpl) IBMFAC(STGADMIN.ADR.STGADMIN.) ACCESS(READ) - ACTION(AUDIT)

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-224050
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224050r877888_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-SM-000020
Rule Title: IBM z/OS DFSMS Program Resources must be properly defined and protected.
Legacy ID: SV-107911
Legacy ID: V-98807

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Check Content:
Refer to the load modules residing in the following Load libraries to determine program resource definitions:
v SYS1.DGTLLIB for DFSMSdfp/ISMF
v SYS1.DGTLLIB for DFSMSdss/ISMF
v SYS1.DFQLLIB for DFSMShsm

If the installation moves these modules to another load library the installation-defined load library must be used in the program protection.

If the TSS resources are owned or DEFPROT is specified for the resource class, this is not a finding.

If the TSS resource access authorizations restrict access to the appropriate personnel, this is not a finding.

Fix Text: Configure the following to be properly specified in the ACP.

Note: The resource type, resources, and/or resource prefixes identified below are examples of a possible installation. The actual resource type, resources, and/or resource prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.

Reference the SMS Program Resources as provided by the following libraries:
v SYS1.DGTLLIB for DFSMSdfp/ISMF
v SYS1.DGTLLIB for DFSMSdss/ISMF
v SYS1.DFQLLIB for DFSMShsm

If the installation moves these modules to another load library the installation-defined load library must be used in the program protection.

The TSS resources as designated in the above are owned and/or DEFPROT is specified for the resource class.

The TSS resource access authorizations restrict access to the appropriate personnel as designated in the above.

The following commands are provided as a sample for implementing resource controls:

Example:
TSS ADD(dept-acid) PROGRAM(ACBFUTO2)
TSS PERMIT(smplsmpl) PROGRAM(ACBFUTO2)
TSS PERMIT(dasdsmpl) PROGRAM(ACBFUTO2)
TSS PERMIT(secasmpl) PROGRAM(ACBFUTO2)
TSS PERMIT(syspsmpl) PROGRAM(ACBFUTO2)
TSS PERMIT(tstcsmpl) PROGRAM(ACBFUTO2)

CCI: CCI-000213

Group ID (Vulid): V-224051
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224051r877889_rule
Severity: CAT II

Rule Version (STIG-ID): TSS0-SM-000030
Rule Title: IBM z/OS DFSMS control data sets must be protected in accordance with security requirements.
Legacy ID: SV-107913
Legacy ID: V-98809

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Check Content:
Refer to the logical parmlib data sets, example: SYS1.PARMLIB(IGDSMSxx), to identify the fully qualified file names for the following SMS data sets:

Source Control Data Set (SCDS)
Active Control Data Set (ACDS)
Communications Data Set (COMMDS)
Automatic Class Selection Routine Source Data Sets (ACS)
ACDS Backup
COMMDS Backup

If the TSS data set rules for the SCDS, ACDS, COMMDS, and ACS data sets restrict UPDATE and ALL access to only systems programming personnel, this is not a finding.

If the TSS data set rules for the SCDS, ACDS, COMMDS, and ACS data sets do not restrict UPDATE and ALL access to only systems programming personnel, this is a finding.

Note: At the discretion of the ISSM, DASD administrators are allowed UPDATE access to the control data sets.

Fix Text: Review the logical parmlib data sets, example: SYS1.PARMLIB(IGDSMSxx), to identify the fully qualified file names for the following SMS data sets:

Source Control Data Set (SCDS)
Active Control Data Set (ACDS)
Communications Data Set (COMMDS)
Automatic Class Selection Routine Source Data Sets (ACS)
ACDS Backup

COMMDS Backup

Assign ownership of the data sets, replacing user-id with a user, department, or division that administer access to the SMS control data sets, and data name with the prefix of the SMS control data sets:

TSS ADD(user-id) DSN(data name)

Ensure the TSS data set rules for the SCDS, ACDS, COMMDS, and ACS data sets restrict UPDATE and ALL access to only z/OS systems programming personnel.

Note: At the discretion of the ISSM, DASD administrators are allowed UPDATE access to the control data sets.

Permit access to those personnel who manage the SMS environment, replacing user-id with the userid of the user or a Group profile:

TSS PERMIT(user-id) DSN(data name) ACC(UPDATE) ACTION(AUDIT)

Permit access to those personnel that perform maintenance on these data sets:

TSS PERMIT(user-id) DSN(data name) ACC(ALL) ACTION(AUDIT)

CCI: CCI-000213

Group ID (Vulid): V-224052
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-224052r877890_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-SM-000040
Rule Title: IBM z/OS using DFSMS must properly specify SYS(x).PARMLIB(IGDSMSxx), SMS parameter settings.
Legacy ID: SV-107915
Legacy ID: V-98811

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the

system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Check Content:
Review the logical parmlib data sets, example: SYS1.PARMLIB(IGDSMSxx), for the following SMS parameter settings:

Parameter Key
SMS
ACDS(ACDS data set name)
COMMDS(COMMDS data set name)

If the required parameters are defined, this is not a finding.

Fix Text: Configure the DFSMS-related PDS members and statements specified in the system parmlib concatenation as outlined below:

Parameter Key
SMS
ACDS(ACDS data set name)
COMMDS(COMMDS data set name)

CCI: CCI-000366

Group ID (Vulid): V-224053
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-224053r877891_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-SM-000050
Rule Title: IBM z/OS DFSMS control data sets must be properly protected.
Legacy ID: SV-107917
Legacy ID: V-98813

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Check Content:

Review the logical parmlib data sets, example: SYS1.PARMLIB(IGDSMSxx), to identify the fully qualified file names for the following SMS data sets:

Source Control Data Set (SCDS)
Active Control Data Set (ACDS)
Communications Data Set (COMMDS)
Automatic Class Selection Routine Source Data Sets (ACS)
ACDS Backup
COMMDS Backup

If the TSS data set rules for the SCDS, ACDS, COMMDS, and ACS data sets restrict UPDATE and ALL access to only systems programming personnel, this is not a finding.

If the TSS data set rules for the SCDS, ACDS, COMMDS, and ACS data sets do not restrict UPDATE and ALL access to only systems programming personnel, this is a finding.

Note: At the discretion of the ISSM, DASD administrators are allowed UPDATE access to the control data sets.

Fix Text: Review the logical parmlib data sets, example: SYS1.PARMLIB(IGDSMSxx), to identify the fully qualified file names for the following SMS data sets:

Source Control Data Set (SCDS)
Active Control Data Set (ACDS)
Communications Data Set (COMMDS)
Automatic Class Selection Routine Source Data Sets (ACS)
ACDS Backup
COMMDS Backup

Assign ownership of the data sets, replacing user-id with a user, department, or division that administer access to the SMS control data sets, and data name with the prefix of the SMS control data sets:

TSS ADD(user-id) DSN(data name)

Ensure the TSS data set rules for the SCDS, ACDS, COMMDS, and ACS data sets restrict UPDATE and ALL access to only z/OS systems programming personnel.

Note: At the discretion of the ISSM, DASD administrators are allowed UPDATE access to the control data sets.

Permit access to those personnel who manage the SMS environment, replacing user-id with the userid of the user or a Group profile:

TSS PERMIT(user-id) DSN(data name) ACC(UPDATE) ACTION(AUDIT)

Permit access to those personnel that perform maintenance on these data sets:

TSS PERMIT(user-id) DSN(data name) ACC(ALL) ACTION(AUDIT)

CCI: CCI-000366

CCI: CCI-000549

Group ID (Vulid): V-224054
Group Title: SRG-OS-000032-GPOS-00013
Rule ID: SV-224054r904400_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-SS-000010
Rule Title: IBM z/OS SMF recording options for the SSH daemon must be configured to write SMF records for all eligible events.
Legacy ID: SV-107919
Legacy ID: V-98815

Vulnerability Discussion: SMF data collection is the basic unit of tracking of all system functions and actions. Included in this tracking data are the audit trails from each of the ACPs. If the control options for the recording of this tracking are not properly maintained, then accountability cannot be monitored, and its use in the execution of a contingency plan could be compromised.

Satisfies: SRG-OS-000032-GPOS-00013, SRG-OS-000392-GPOS-00172

Check Content:
Locate the SSH daemon configuration file, which may be found in /etc/ssh/ directory.

Alternately:
From UNIX System Services ISPF Shell, navigate to ribbon select tools.
Select option 1 - Work with Processes.

If SSH Daemon is not active, this is not a finding.

Examine SSH daemon configuration file.

If ServerSMF is not coded with ServerSMF TYPE119_U83 or is commented out, this is a finding.

Fix Text: Configure the SERVERSMF statement in the SSH Daemon configuration file to

TYPE119_U83.

CCI: CCI-000067

CCI: CCI-002884

Group ID (Vulid): V-224055
Group Title: SRG-OS-000228-GPOS-00088
Rule ID: SV-224055r877893_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-SS-000040
Rule Title: The IBM z/OS SSH daemon must be configured with the Standard Mandatory DoD Notice and Consent Banner.
Legacy ID: V-98817
Legacy ID: SV-107921

Vulnerability Discussion: Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read & consent to terms in IS user agreem't."

Check Content:
Locate the SSH daemon configuration file.
May be found in /etc/ssh/ directory.

Alternately:
From UNIX System Services ISPF Shell navigate to ribbon select tools.
Select option 1 - Work with Processes.

If SSH Daemon is not active, this is not a finding.

Examine SSH daemon configuration file.

If Banner statement is missing or configured to none, this is a finding.

Ensure that the contents of the file specified on the banner statement contain a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. If there is any deviation this is a finding.

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Fix Text: Configure the banner statement to a file that contains the Department of Defense (DoD) logon banner.

Ensure that the contents of the file specified on the banner statement contain a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer.

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy,

and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

Group ID (Vulid): V-224056
Group Title: SRG-OS-000032-GPOS-00013
Rule ID: SV-224056r877896_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-TC-000010
Rule Title: IBM z/OS PROFILE.TCPIP configuration statements for the TCP/IP stack must be properly coded.
Legacy ID: V-98819
Legacy ID: SV-107923

Vulnerability Discussion: Remote access services, such as those providing remote access to network devices and information systems, which lack automated monitoring capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Automated monitoring of remote access sessions allows organizations to detect cyberattacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote access capabilities, such as Remote Desktop Protocol (RDP), on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Check Content:
Refer to the Profile configuration file specified on the PROFILE DD statement in the TCPIP

started task JCL.

If the following items are in effect for the configuration statements specified in the TCP/IP Profile configuration file, this is not a finding.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

-The SMFPARMS statement is not coded or commented out.
-The DELETE statement is not coded or commented out for production systems.
-The SMFCONFIG statement is coded with (at least) the FTPCLIENT and TN3270CLIENT operands.
-The TCPCONFIG and UDPCONFIG statements are coded with (at least) the RESTRICTLOWPORTS operand.

If the TCPCONFIG does not have the TTLS statement coded, this is a finding.

NOTE: If the INCLUDE statement is coded, the data set specified will be checked for access authorization compliance.

Fix Text: Ensure the following items are in effect for the configuration statements specified in the TCP/IP Profile configuration file:

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

-The SMFPARMS statement is not coded or commented out.
-The DELETE statement is not coded or commented out for production systems.
-The SMFCONFIG statement is coded with (at least) the FTPCLIENT and TN3270CLIENT operands.
-The TCPCONFIG and UDPCONFIG statements are coded with (at least) the RESTRICTLOWPORTS operand.

NOTE: If the INCLUDE statement is coded, the data set specified will be checked for access authorization compliance in STIG ID ITCP0070.

BASE TCP/IP PROFILE.TCPIP CONFIGURATION STATEMENTS
FUNCTIONS

INCLUDE- Specifies the name of an MVS data set that contains additional PROFILE.TCPIP statements to be used
- Alters the configuration specified by previous statements

SMFPARMS- Specifies SMF logging options for some TCP applications; replaced by SMFCONFIG
- Controls collection of audit data

DELETE- Specifies some previous statements, including PORT and PORTRANGE, that are to be deleted
- Alters the configuration specified by previous statements

SMFCONFIG- Specifies SMF logging options for Telnet, FTP, TCP, API, and stack activity
- Controls collection of audit data

TCPCONFIG- Specifies various settings for the TCP protocol layer of TCP/IP
- Controls port access

TCPCONFIG coded with TTLS - Specifies that the AT-TLS function is activated for the TCP/IP stack. The AT-TLS function provides invocation of System SSL in the TCP transport layer of the stack.

Note: If AT-TLS is enabled, you must activate the SERVAUTH class, define the INITSTACK resource profile, and permit users to it.

NOTE: If the INCLUDE statement is coded, the data set specified will be checked for access authorization compliance.

CCI: CCI-000067

Group ID (Vulid): V-224057
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224057r877897_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-TC-000020
Rule Title: IBM z/OS permission bits and user audit bits for HFS objects that are part of the Base TCP/IP component must be configured properly.
Legacy ID: V-98821
Legacy ID: SV-107925

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
From the ISPF Command Shell enter:
omvs

At the input line enter:
cd /etc
enter
ls -alW

If the following File permission and user Audit Bits are true this is not a finding.

/etc/hosts 0744 faf
/etc/protocol 0744 faf
/etc/resolv.conf 0744 faf
/etc/services 0740 faf

cd /usr
ls -alW

If the following file permission and user Audit Bits are true this is not a finding.

/usr/lpp/tcpip/sbin 0755 faf
/usr/lpp/tcpip/bin 0755 faf

Notes: Some of the files listed above are not used in every configuration. The absence of a file is not considered a finding.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
- no auditing

Fix Text: With the assistance of a systems programmer with UID(0) and/or SUPERUSER access, configure the UNIX permission bits and user audit bits on the HFS directories and files for the FTP Server to conform to the specifications in the table below:

BASE TCP/IP HFS Object Security Settings
File Permission Bits User Audit Bits
/etc/hosts 0744 faf
/etc/protocol 0744 faf
/etc/resolv.conf 0744 faf
/etc/services 0740 faf
/usr/lpp/tcpip/sbin 0755 faf
/usr/lpp/tcpip/bin 0755 faf

Some of the files listed above (e.g., /etc/resolv.conf) are not used in every configuration. While the absence of a file is generally not a security issue, the existence of a file that has not been properly secured can often be an issue. Therefore, all directories and files that do exist will have the specified permission and audit bit settings.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
- no auditing

The following commands can be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

chmod 0744 /etc/hosts
chaudit w=sf,rx+f /etc/hosts
chmod 0744 /etc/protocol

chaudit w=sf,rx+f /etc/protocol
chmod 0744 /etc/resolv.conf
chaudit w=sf,rx+f /etc/resolv.conf
chmod 0740 /etc/services
chaudit w=sf,rx+f /etc/services
chmod 0755 /usr/lpp/tcpip/bin
chaudit w=sf,rx+f /usr/lpp/tcpip/bin
chmod 0755 /usr/lpp/tcpip/sbin
chaudit w=sf,rx+f /usr/lpp/tcpip/sbin

CCI: CCI-000213

Group ID (Vulid): V-224058
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224058r877898_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-TC-000030
Rule Title: IBM z/OS TCP/IP resources must be properly protected.
Legacy ID: SV-107927
Legacy ID: V-98823

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Check Content:
If the following guidance is true, this is not a finding.

-The EZA, EZB, and IST resources of the SERVAUTH resource class are properly owned and/or DEFPROT is specified in the SERVAUTH resource class.
-No access is given to the EZA, EZB, and IST high level resources of the SERVAUTH resource class.
-If the product CSSMTP is on the system, no access is given to EZB.CSSMTP of the SERVAUTH resource class.
-If the product CSSMTP is on the system, EZB.CSSMTP.sysname.writername.JESnode will be specified and made available to the CSSMTP started task and authenticated users that require

access to use CSSMTP for e-mail services.
-Authenticated users that require access will be permitted access to the second level of the resources in the SERVAUTH resource class. Examples are the network (NETACCESS), port (PORTACCESS), stack (STACKACCESS), and FTP resources in the SERVAUTH resource class.
-The EZB.STACKACCESS. resource access authorizations restrict access to those started tasks with valid requirements and users with valid FTP access requirements.
-The EZB.FTP.*.*.ACCESS.HFS) resource access authorizations restrict access to FTP users with specific written documentation showing a valid requirement exists to access OMVS files and directories.
-The EZB.INITSTACK.sysname.tcpname resource access authorizations restrict access before policies have been installed, to users authorized by the system security plan requiring access to the TCP/IP stack.

Fix Text: Develop a plan of action to implement the required changes. Ensure the following items are in effect for TCP/IP resources.

Note: The resource class, resources, and/or resource prefixes identified below are examples of a possible installation. The actual resource class, resources, and/or resource prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.

-Ensure that the EZA, EZB, and IST resources of the SERVAUTH resource class are properly owned and/or DEFPROT is specified in the SERVAUTH resource class.
-No access is given to the EZA, EZB, and IST resources of the SERVAUTH resource class.
-If the product CSSMTP is on the system, no access is given to EZB.CSSMTP of the SERVAUTH resource class. EZB.CSSMTP.sysname.writername.JESnode will be specified and made available to the CSSMTP started task and authenticated users that require access to use CSSMTP for e-mail services.
-Only authenticated users that require access are permitted access to the second level of the resources in the SERVAUTH resource class. Examples are the network (NETACCESS), port (PORTACCESS), stack (STACKACCESS), and FTP resources in the SERVAUTH resource class.
-The EZB.STACKACCESS. resource access authorizations restrict access to those started tasks with valid requirements and users with valid FTP access requirements.
-The EZB.FTP.*.*.ACCESS.HFS) resource access authorizations restrict access to FTP users with specific written documentation showing a valid requirement exists to access OMVS files and Directories.

The EZB.INITSTACK.sysname.tcpname resource access authorizations restrict access to TCP/IP stack before policies have been installed to users authorized by the system security plan.

The following commands are provided as a sample for implementing resource controls:

TSS ADD(ADMIN) SERVAUTH(EZB)
or

TSS REPLACE(RDT) RESCLASS(SERVAUTH) ATTR(DEFPROT)

TSS PER(authusers) SERVAUTH(EZB.CSSMTP.sysname.writername.JESnode) ACCESS(READ)
TSS PER(authusers) SERVAUTH(EZB.FTP.) ACCESS(READ)
TSS PER(ftpprofile)SERVAUTH(EZB.FTP.sysname.ftpstc.ACCESS.HFS)ACC(READ)
TSS PER(authusers) SERVAUTH(EZB.NETACCESS.) ACCESS(READ)
TSS PER(authusers) SERVAUTH(EZB.PORTACCESS.) ACCESS(READ)
TSS PER(authusers) SERVAUTH(EZB.STACKACCESS.) ACCESS(READ)
TSS PER(authusers) SERVAUTH(EZB.INITSTACK.) ACCESS(READ)

TSS PER(ftpprofile)SERVAUTH(EZB.STACKACCESS.sysname.TCPIP)ACC(READ)

CCI: CCI-000213

Group ID (Vulid): V-224059
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224059r877899_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-TC-000040
Rule Title: IBM z/OS data sets for the Base TCP/IP component must be properly protected.
Legacy ID: SV-107929
Legacy ID: V-98825

Vulnerability Discussion: MVS data sets of the Base TCP/IP component provide the configuration, operational, and executable properties of IBMs TCP/IP system product. Failure to properly secure these data sets may lead to unauthorized access resulting in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices,

files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100

Check Content:
Execute a data set access list for all TCP/IP base components.

If all of the following items are true, this is not a finding.

WRITE and ALLOCATE access to product data sets is restricted to systems programming personnel (i.e., SMP/E distribution data sets with the prefix SYS1.TCPIP.AEZA and target data sets with the prefix SYS1.TCPIP.SEZA).

WRITE and ALLOCATE access to the data set(s) containing the Data and Profile configuration files is restricted to systems programming personnel.

Note: If any INCLUDE statements are specified in the Profile configuration file, the named MVS data sets have the same access authorization requirements.

WRITE and ALLOCATE access to the data set(s) containing the Data and Profile configuration files is logged.

Note: If any INCLUDE statements are specified in the Profile configuration file, the named MVS data sets have the same logging requirements.

WRITE and ALLOCATE access to the data set(s) containing the configuration files shared by TCP/IP applications is restricted to systems programming personnel.

Note: For systems running the TSS ACP replace the WRITE and ALLOCATE with WRITE, UPDATE, CREATE, CONTROL, SCRATCH, and ALL.

Fix Text: Review the data set access authorizations defined to the ACP for the Base TCP/IP component. Configure these data sets to be protected in accordance with the following rules:

WRITE and ALLOCATE access to product data sets is restricted to systems programming personnel (i.e., SMP/E distribution data sets with the prefix SYS1.TCPIP.AEZA and target data sets with the prefix SYS1.TCPIP. SEZA).

WRITE and ALLOCATE access to the data set(s) containing the Data and Profile configuration files is restricted to systems programming personnel.

Note: If any INCLUDE statements are specified in the Profile configuration file, the named MVS data sets have the same access authorization requirements.

WRITE and ALLOCATE access to the data set(s) containing the Data and Profile configuration

files is logged.

Note: If any INCLUDE statements are specified in the Profile configuration file, the named MVS data sets have the same logging requirements.

WRITE and ALLOCATE access to the data set(s) containing the configuration files shared by TCP/IP applications is restricted to systems programming personnel.

Note: For systems running the TSS ACP replace the WRITE and ALLOCATE with WRITE, UPDATE, CREATE, CONTROL, SCRATCH, and ALL.

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-224060
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-224060r877900_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-TC-000050
Rule Title: IBM z/OS Configuration files for the TCP/IP stack must be properly specified.
Legacy ID: SV-107931
Legacy ID: V-98827

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Check Content:
Refer to the procedure libraries defined to JES2 and locate the TCPIP JCL member.

Note:

If GLOBALTCPIPDATA is specified, any TCPIP.DATA statements contained in the specified file or data set take precedence over any TCPIP.DATA statements found using the appropriate environment's (native MVS or z/OS UNIX) search order.

If GLOBALTCPIPDATA is not specified, the appropriate environment's (Native MVS or z/OS UNIX) search order is used to locate TCPIP.DATA.

If the PROFILE and SYSTCPD DD statements specify the TCP/IP Profile and Data configuration files respectively, this not a finding.

If the RESOLVER_CONFIG variable on the EXEC statement is set to the same file name specified on the SYSTCPD DD statement, this is not a finding.

Fix Text: Review the TCP/IP started task JCL to ensure the configuration file names are specified on the appropriate DD statements and parameter option.

During initialization, the TCP/IP stack uses fixed search sequences to locate the PROFILE.TCPIP and TCPIP.DATA files. However, uncertainty is reduced and security auditing is enhanced by explicitly specifying the locations of the files. In the TCP/IP started task's JCL, Data Definition (DD) statements can be used to specify the locations of the files. The PROFILE DD statement identifies the PROFILE.TCPIP file and the SYSTCPD DD statement identifies the TCPIP.DATA file.

The location of the TCPIP.DATA file can also be specified by coding the RESOLVER_CONFIG environment variable as a parameter of the ENVAR option in the TCP/IP started task's JCL. In fact, the value of this variable is checked before the SYSTCPD DD statement by some processes. However, not all processes (e.g., TN3270 Telnet Server) will access the variable to get the file location. Therefore, specifying the file location explicitly, both on a DD statement and through the RESOLVER_CONFIG environment variable, reduces ambiguity.

Note:
If GLOBALTCPIPDATA is specified, any TCPIP.DATA statements contained in the specified file or data set take precedence over any TCPIP.DATA statements found using the appropriate environment's (native MVS or z/OS UNIX) search order.

If GLOBALTCPIPDATA is not specified, the appropriate environment's (Native MVS or z/OS UNIX) search order is used to locate TCPIP.DATA.

The systems programmer responsible for supporting ICS will ensure that the TCP/IP started task's JCL specifies the PROFILE and SYSTCPD DD statements for the PROFILE.TCPIP and TCPIP.DATA configuration files and TCP/IP started task's JCL includes the RESOLVER_CONFIG variable, set to the name of the file specified on the SYSTCPD DD statement.

CCI: CCI-000366

Group ID (Vulid): V-224061
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-224061r877901_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-TC-000060
Rule Title: IBM z/OS started tasks for the Base TCP/IP component must be defined in accordance with security requirements.
Legacy ID: V-98829
Legacy ID: SV-107933

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
Refer to system Proclibs to determine the TCPIP address space(s).

From the ISPF Command Shell enter:
TSS list(<TCPIP STCs>) SEGMENT(OMVS)

For each TCPIP:

If all of the following items are true, this is not a finding.

If any item is untrue, this is a finding.

From the ISPF Command Shell enter
TSS LIST(EZAZSSI) SEGMENT(OMVS)

If EZAZSSI STC has the STC facility, this is not finding.

-Named TCPIP or, in the case of multiple instances, prefixed with TCPIP.
-Has the STC facility.

-z/OS UNIX attributes:
UID(0), HOME directory '/', shell program /bin/sh

Ensure the following items are in effect for the ACID assigned to the EZAZSSI started task:
-Named EZAZSSI
-Has the STC facility.

Fix Text: Develop a plan of action to implement the required changes. Ensure the following items are in effect for the ACID(s) assigned to the TCP/IP address space(s):

1) Named TCPIP or, in the case of multiple instances, prefixed with TCPIP

2) Has the STC facility

3) z/OS UNIX attributes: UID(0), HOME directory '/', shell program /bin/sh

Ensure the following items are in effect for the ACID assigned to the EZAZSSI started task:

1) Named EZAZSSI

2) Has the STC facility

For example:

The following commands can be used to create the user accounts and assign the privileges that are required for the TCP/IP address space and the EZAZSSI started task:

TSS CREATE(TCPIP) TYPE(USER) NAME(TCPIP)
DEPT(existing-dept) FACILITY(STC) PASSWORD(password,0)
TSS ADD(TCPIP) DFLTGRP(STCTCPX) GROUP(STCTCPX)
TSS ADD(TCPIP) SOURCE(INTRDR)
TSS ADD(TCPIP) UID(0) HOME(/) OMVSPGM(/bin/sh)
TSS ADD(TCPIP) MASTFAC(TCP)
TSS ADD(STC) PROCNAME(TCPIP) ACID(TCPIP)
TSS PERMIT(TCPIP) IBMFAC(BPX.DAEMON) ACCESS(READ)

TSS CREATE(EZAZSSI) TYPE(USER) NAME(EZAZSSI)
DEPT(existing-dept) FACILITY(STC) PASSWORD(password,0)
TSS ADD(EZAZSSI) DFLTGRP(STCTCPX) GROUP(STCTCPX)
TSS ADD(EZAZSSI) SOURCE(INTRDR)
TSS ADD(EZAZSSI) UID(non-zero) HOME(/) OMVSPGM(/bin/sh)

TSS ADD(EZAZSSI) MASTFAC(TCP)
TSS ADD(STC) PROCNAME(EZAZSSI) ACID(EZAZSSI)

CCI: CCI-000764

Group ID (Vulid): V-224062
Group Title: SRG-OS-000297-GPOS-00115
Rule ID: SV-224062r877902_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-TC-000070
Rule Title: IBM z//OS must be configured to restrict all TCP/IP ports to ports, protocols, and/or services as defined in the PPSM CAL and vulnerability assessments.
Legacy ID: SV-107935
Legacy ID: V-98831

Vulnerability Discussion: Remote access services, such as those providing remote access to network devices and information systems, which lack automated control capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Operating system functionality (e.g., RDP) must be capable of taking enforcement action if the audit reveals unauthorized activity. Automated control of remote access sessions allows organizations to ensure ongoing compliance with remote access policies by enforcing connection rules of remote access applications on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Check Content:
Refer the TCPIP PROFILE DD statement to determine the TCP/IP Ports. If the PROFILE DD statement is not supplied use the default search order to find thee PROFILE data set. See the IP Configuration Guide for a description of the search order for PROFILE.TCPIP.

If the all the Ports included into the configuration are restricted to the ports, protocols, and/or services, as defined in the Ports, Protocols, and Services Management (PPSM) Category Assurance List (CAL) and vulnerability assessments, this is not a finding.

Fix Text: Configure TCP/IP PROFILE port definitions to adhere to ports, protocols, and/or services, as defined in the Ports, Protocols, and Services Management (PPSM) Category Assurance List (CAL) and vulnerability assessments.

CCI: CCI-002314

Group ID (Vulid): V-245537
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-245537r877948_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-TC-000080
Rule Title: The IBM z/OS TCPIP.DATA configuration statement must contain the DOMAINORIGIN or DOMAIN specified for each TCP/IP defined.
Legacy ID: SV-107937
Legacy ID: V-98833

Vulnerability Discussion: If data origin authentication and data integrity verification are not performed, the resultant response could be forged, it may have come from a poisoned cache, the packets could have been intercepted without the resolver's knowledge, or resource records could have been removed which would result in query failure or denial of service. Data origin authentication verification must be performed to thwart these types of attacks.

Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching Domain Name System (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations.

This is not applicable if DNSSEC is not implemented on the local network.

Check Content:
Refer to the Data configuration file specified on the SYSTCPD DD statement in the TCPIP started task JCL.

Note:
If GLOBALTCPIPDATA is specified, any TCPIP.DATA statements contained in the specified file or data set take precedence over any TCPIP.DATA statements found using the appropriate environment's (native MVS or z/OS UNIX) search order.

If GLOBALTCPIPDATA is not specified, the appropriate environment's (Native MVS or z/OS UNIX) search order is used to locate TCPIP.DATA.

If the DOMAINORIGIN/DOMAIN (The DOMAIN statement is functionally equivalent to the DOMAINORIGIN Statement) is specified in the TCP/IP Data configuration file, this is not a

finding.

Fix Text: Configure the TCPIP.DATA file to include the DOMAINORIGIN/DOMAIN (The DOMAIN statement is functionally equivalent to the DOMAINORIGIN Statement).

Note:
If GLOBALTCPIPDATA is specified, any TCPIP.DATA statements contained in the specified file or data set take precedence over any TCPIP.DATA statements found using the appropriate environment's (native MVS or z/OS UNIX) search order.

If GLOBALTCPIPDATA is not specified, the appropriate environment's (Native MVS or z/OS UNIX) search order is used to locate TCPIP.DATA.

CCI: CCI-000366

Group ID (Vulid): V-252554
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-252554r816962_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-TC-000100
Rule Title: IBM z/OS TCP/IP AT-TLS policy must be properly configured in Policy Agent.

Vulnerability Discussion: If events associated with nonlocal administrative access or diagnostic sessions are not logged, a major tool for assessing and investigating attacks would not be available.

This requirement addresses auditing-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems.

Nonlocal maintenance and diagnostic activities are conducted by individuals communicating through an external network (e.g., the internet) or an internal network. Local maintenance and diagnostic activities are carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

This requirement applies to hardware/software diagnostic test equipment or tools. This requirement does not cover hardware/software components that may support information system maintenance, yet are a part of the system; for example, the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch.

Check Content:
Use the z/OS UNIX pasearch -t command to query information from the z/OS UNIX Policy

Agent.

The command is issued from the UNIX System Services shell.

Examine the results for AT-TLS initiation and control statements.

If there are no AT-TLS initiation and controls statements, this is a finding.

Verify the statements specify a FIPS 140-2 compliant value. If none of the following values are present, this is a finding

ECDHE_ECDSA_AES_128_CBC_SHA256
ECDHE_ECDSA_AES_256_CBC_SHA384
ECDHE_RSA_AES_128_CBC_SHA256
ECDHE_RSA_AES_256_CBC_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256

Fix Text: Develop a plan of action to implement the required changes. Ensure the following items are in effect for TCP/IP resources.

Develop AT-TLS policy. Install in the policy agent.

Ensure the statements specify a FIPS 140-2 compliant value of the following values.

ECDHE_ECDSA_AES_128_CBC_SHA256
ECDHE_ECDSA_AES_256_CBC_SHA384
ECDHE_RSA_AES_128_CBC_SHA256
ECDHE_RSA_AES_256_CBC_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256

CCI: CCI-000067

Group ID (Vulid): V-224065
Group Title: SRG-OS-000023-GPOS-00006
Rule ID: SV-224065r877903_rule
Severity: CAT II

Rule Version (STIG-ID): TSS0-TN-000010
Rule Title: IBM z/OS TN3270 Telnet server configuration statement MSG10 text must have the Standard Mandatory DoD Notice and Consent Banner.
Legacy ID: V-98837
Legacy ID: SV-107941

Vulnerability Discussion: Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read & consent to terms in IS user agreem't."

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007

Check Content:
Refer to the Profile configuration file specified on the PROFILE DD statement in the TN3270 started task JCL.

If all USS tables referenced in BEGINVTAM USSTCP statements include MSG10 text that specifies the Standard logon banner this is not a finding.

The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

DOD requires that a logon warning banner be displayed. Within the TN3270 Telnet Server, the

banner can be implemented through the USS table that is specified on a BEGINVTAM USSTCP statement. The text associated with message ID 10 (i.e., MSG10) in the USS table is sent to clients that are subject to USSTCP processing.

Fix Text: Review all USS tables referenced in BEGINVTAM USSTCP statements in the PROFILE.TCPIP file. Ensure the MSG10 text specifies a logon banner in accordance with DISA requirements. See MGG10 below:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

DOD requires that a logon warning banner be displayed. Within the TN3270 Telnet Server, the banner can be implemented through the USS table that is specified on a BEGINVTAM USSTCP statement. The text associated with message ID 10 (i.e., MSG10) in the USS table is sent to clients that are subject to USSTCP processing.

CCI: CCI-000048

CCI: CCI-000050

Group ID (Vulid): V-224066
Group Title: SRG-OS-000392-GPOS-00172
Rule ID: SV-224066r877904_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-TN-000020
Rule Title: IBM z/OS SMF recording options for the TN3270 Telnet server must be properly specified.
Legacy ID: V-98839
Legacy ID: SV-107943

Vulnerability Discussion: Remote access services, such as those providing remote access to network devices and information systems, which lack automated monitoring capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Automated monitoring of remote access sessions allows organizations to detect cyberattacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote access capabilities, such as Remote Desktop Protocol (RDP), on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000032-GPOS-00013

Check Content:
Refer to the Profile configuration file specified on the PROFILE DD statement in the TCPIP started task JCL.

If the following configuration statement settings are in effect in the TCP/IP Profile configuration data set, this is not a finding.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration data set, the data set specified on this statement must be checked for the following items as well.

-The TELNETPARMS SMFINIT statement is coded with the TYPE119 operand within each TELNETPARMS statement block.
-The TELNETPARMS SMFTERM statement is coded with the TYPE119 operand within each TELNETPARMS statement block.

Note: The SMFINIT and SMFTERM statement can appear in both TELNETGLOBAL and TELNETPARM statement blocks. If duplicate statements appear in the TELNETGLOBALS,

TELNETPARMS, Telnet uses the last valid statement that was specified.

Fix Text: Code TN3270 configuration file to the requirements specified below.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

-The TELNETPARMS SMFINIT statement is coded with the TYPE119 operand within each TELNETPARMS statement block.
-The TELNETPARMS SMFTERM statement is coded with the TYPE119 operand within each TELNETPARMS statement block.

NOTE: Effective in z/OS release 1.2, the SMFINIT and SMFTERM statement can appear in both TELNETGLOBAL and TELNETPARM statement blocks.

CCI: CCI-000067

CCI: CCI-002884

Group ID (Vulid): V-224067
Group Title: SRG-OS-000033-GPOS-00014
Rule ID: SV-224067r877905_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-TN-000030
Rule Title: IBM z/OS SSL encryption options for the TN3270 Telnet server must be specified properly for each statement that defines a SECUREPORT or within the TELNETGLOBALS.
Legacy ID: V-98841
Legacy ID: SV-107945

Vulnerability Discussion: Without confidentiality protection mechanisms, unauthorized individuals may gain access to sensitive information via a remote access session.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Encryption provides a means to secure the remote connection to prevent unauthorized access to the data traversing the remote access connection (e.g., RDP), thereby providing a degree of confidentiality. The encryption strength of a mechanism is selected based on the security categorization of the information.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000120-GPOS-00061, SRG-OS-000250-

GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000396-GPOS-00176, SRG-OS-000478-GPOS-00223, SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190, SRG-OS-000478-GPOS-00223

Check Content:
Refer to the Profile configuration file specified on the PROFILE DD statement in the TCPIP started task JCL.
If the following items are in effect for the configuration specified in the TCP/IP Profile configuration file, this is not a finding.
NOTE: If an INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

NOTE: FIPS 140-2 minimum encryption is the accepted level of encryption and will override this requirement if greater.

-The TELNETGLOBALS block that specifies an ENCRYPTION statement states one or more of the below cipher specifications.
-Each TELNETPARMS block that specifies the SECUREPORT statement, specifies an ENCRYPTION statement states one or more of the below cipher specifications. And the TELNETGLOBALS block does or does not specify an ENCRYPTION statement.

Cipher Specifications
SSL_3DES_SHA
SSL_AES_256_SHA
SSL_AES_128_SHA

Fix Text: Configure the SECUREPORT and TELNETPARMS ENCRYPTION statements and/or the TELNETGLOBALS statement in the PROFILE.TCPIP file to conform to the requirements specified below.

The TELNETGLOBALS block may specify an ENCRYPTION statement that specifies one or more of the below cipher specifications.

Each TELNETPARMS block that specifies the SECUREPORT statement, an ENCRYPTION statement is coded with one or more of the below cipher specifications. And the TELNETGLOBALS block does or does not specify an ENCRYPTION statement.

To prevent the use of non FIPS 140-2 encryption, the TELNETGLOBALS block and/or each TELNETPARMS block that specifies an ENCRYPTION statement will specify one or more of the following cipher specifications:

Cipher Specifications
SSL_3DES_SHA
SSL_AES_256_SHA

SSL_AES_128_SHA

Note: Always check for the minimum allowed in FIPS 140-2.

CCI: CCI-000068

CCI: CCI-000803

CCI: CCI-001453

CCI: CCI-002418

CCI: CCI-002420

CCI: CCI-002421

CCI: CCI-002422

CCI: CCI-002450

CCI: CCI-002890

CCI: CCI-003123

Group ID (Vulid): V-224068
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-224068r877906_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-TN-000040
Rule Title: IBM z/OS VTAM session setup controls for the TN3270 Telnet server must be properly specified.
Legacy ID: V-98843
Legacy ID: SV-107947

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Check Content:
Refer to the TN3270 Profile configuration file identified by the PROFILE DD in the TN3270 procedure.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

If all of the following are true, this is not a finding.

If any of the above is untrue, this is a finding.

-Within each BEGINVTAM statement block, one BEGINVTAM USSTCP statement is coded that specifies only the table name operand. No client identifier, such as host name or IP address, is specified so the statement applies to all connections not otherwise controlled.
-The USS table specified on each "back stop" USSTCP statement mentioned in Item (1) above is coded to allow access only to session manager applications and NC PASS applications.
-Within each BEGINVTAM statement block, additional BEGINVTAM USSTCP statements that specify a USS table that allows access to other applications may be coded only if the statements include a client identifier operand that references only secure terminals.
-Any BEGINVTAM DEFAULTAPPL statement that does not specify a client identifier, or specifies any type of client identifier that would apply to unsecured terminals, specifies a session manager application or an NC PASS application as the application name.
-Any BEGINVTAM LUMAP statement, if used with the DEFAPPL operand and applied to unsecured terminals, specifies only a session manager application or an NC PASS application.

NOTE: The BEGINVTAM LINEMODEAPPL requirements will not be reviewed at this time. Further testing must be performed to determine how the CL/Supersession and NC-PASS applications work with line mode.

Fix Text: Review the BEGINVTAM configuration statements in the PROFILE.TCPIP file. Ensure they conform to the specifications below.

NOTE: If the INCLUDE statement is coded in the TN3270 Profile configuration file, the data set specified on this statement must be checked for the following items as well.

Within each BEGINVTAM statement block, one BEGINVTAM USSTCP statement is coded that specifies only the table name operand. No client identifier, such as host name or IP address, is specified so the statement applies to all connections not otherwise controlled.

The USS table specified on each "back stop" USSTCP statement mentioned above is coded to allow access only to session manager applications and NC PASS applications.

Within each BEGINVTAM statement block, additional BEGINVTAM USSTCP statements that specify a USS table that allows access to other applications may be coded only if the statements include a client identifier operand that references only secure terminals.

Any BEGINVTAM DEFAULTAPPL statement that does not specify a client identifier, or specifies any type of client identifier that would apply to unsecured terminals, specifies a session manager application or an NC PASS application as the application name.

CCI: CCI-000366

Group ID (Vulid): V-224069
Group Title: SRG-OS-000163-GPOS-00072
Rule ID: SV-224069r877907_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-TN-000050
Rule Title: IBM z/OS PROFILE.TCPIP configuration for the TN3270 Telnet server must have the INACTIVE statement properly specified.
Legacy ID: V-98845
Legacy ID: SV-107949

Vulnerability Discussion: Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Check Content:
Refer to the Profile configuration file specified on the PROFILE DD statement in the TCPIP started task JCL.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

TELNETPARMS Block (one defined for each port the server is listening to, typically ports 23 and 992)

If the TELNETPARMS INACTIVE statement is coded within each TELNETPARMS statement block and specifies a value between "1" and "900", this is not a finding.

NOTE: Effective in z/OS release 1.2, the INACTIVE statement can appear in both TELNETGLOBAL and TELNETPARM statement blocks.

Fix Text: Configure the configuration statements in the PROFILE.Tn3270 to conform to the specifications below:

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

The TELNETPARMS INACTIVE statement is coded either within the TELNETGLOBALS or within each TELNETPARMS statement block and specifies a value between "1" and "900".

CCI: CCI-001133

CCI: CCI-002361

Group ID (Vulid): V-224070
Group Title: SRG-OS-000228-GPOS-00088
Rule ID: SV-224070r877908_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-TN-000060
Rule Title: The IBM z/OS warning banner for the TN3270 Telnet server must be properly specified.
Legacy ID: V-98847
Legacy ID: SV-107951

Vulnerability Discussion: Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and

are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read & consent to terms in IS user agreem't."

Check Content:
Refer to the Profile configuration file specified on the PROFILE DD statement in the TN3270 started task JCL.

If all USS tables referenced in BEGINVTAM USSTCP statements include MSG10 text that specifies the Standard logon banner, this is not a finding.

The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD

information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

DOD requires that a logon warning banner be displayed. Within the TN3270 Telnet Server, the banner can be implemented through the USS table that is specified on a BEGINVTAM USSTCP statement. The text associated with message ID 10 (i.e., MSG10) in the USS table is sent to clients that are subject to USSTCP processing.

Fix Text: Review all USS tables referenced in BEGINVTAM USSTCP statements in the PROFILE.TCPIP file. Ensure the MSG10 text specifies a logon banner in accordance with DISA requirements. See MGG10 below:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

DOD requires that a logon warning banner be displayed. Within the TN3270 Telnet Server, the banner can be implemented through the USS table that is specified on a BEGINVTAM USSTCP statement. The text associated with message ID 10 (i.e., MSG10) in the USS table is sent to clients that are subject to USSTCP processing.

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

Group ID (Vulid): V-224071
Group Title: SRG-OS-000425-GPOS-00189
Rule ID: SV-224071r877909_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-TN-000070

Rule Title: IBM z/OS TELNETPARMS or TELNETGLOBALS must specify a SECUREPORT statement for systems requiring confidentiality and integrity.
Legacy ID: SV-107953
Legacy ID: V-98849

Vulnerability Discussion: Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission, for example, during aggregation, at protocol transformation points, and during packing/unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

Ensuring the confidentiality of transmitted information requires the operating system to take measures in preparing information for transmission. This can be accomplished via access control and encryption.

Use of this requirement will be limited to situations where the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process. When transmitting data, operating systems need to support transmission protection mechanisms such as TLS, SSL VPNs, or IPsec.

Satisfies: SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Check Content:
Refer to the Profile configuration file specified on the PROFILE DD statement in the TCPIP started task JCL.

If the following items are in effect for the configuration specified in the TCP/IP Profile configuration file, this is not a finding.

NOTE: If an INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

NOTE: FIPS 140-2 minimum encryption is the accepted level of encryption and will override this requirement if greater.

-The TELNETGLOBALS block that specifies an ENCRYPTION statement states one or more of the below cipher specifications.
-Each TELNETPARMS block that specifies the SECUREPORT statement, specifies an ENCRYPTION statement states one or more of the below cipher specifications. And the TELNETGLOBALS block does or does not specify an ENCRYPTION statement.

Cipher Specifications
SSL_3DES_SHA
SSL_AES_256_SHA
SSL_AES_128_SHA

Fix Text: Configure the SECUREPORT and TELNETPARMS ENCRYPTION statements and/or the TELNETGLOBALS statement in the PROFILE.TCPIP file to conform to the requirements specified below.

The TELNETGLOBALS block may specify an ENCRYPTION statement that specifies one or more of the below cipher specifications.

Each TELNETPARMS block that specifies the SECUREPORT statement, an ENCRYPTION statement is coded with one or more of the below cipher specifications. And the TELNETGLOBALS block does or does not specify an ENCRYPTION statement.

To prevent the use of non FIPS 140-2 encryption, the TELNETGLOBALS block and/or each TELNETPARMS block that specifies an ENCRYPTION statement will specify one or more of the following cipher specifications:

Cipher Specifications
SSL_3DES_SHA
SSL_AES_256_SHA
SSL_AES_128_SHA

Note: Always check for the minimum allowed in FIPS 140-2.

CCI: CCI-002420

CCI: CCI-002422

Group ID (Vulid): V-224072
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224072r877910_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-TS-000010
Rule Title: IBM Z/OS TSOAUTH resources must be restricted to authorized users.
Legacy ID: SV-107955
Legacy ID: V-98851

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and

current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
From the ISPF Command Shell enter:
TSS WHOOWNS TSOAUTH(*)

For each resource defined enter:
TSS WHOHAS(<tsoauth resource>)

If the following guidance is true, this is not a finding.

-The ACCT authorization is restricted to security personnel.
-The CONSOLE authorization is restricted to authorized systems personnel (e.g., systems programming personnel, operations staff, etc.) and READ access may be given to all user when SDSF in install at the ISSOs discretion.
-The MOUNT authorization is restricted to DASD batch users only.
-The OPER authorization is restricted to authorized systems personnel (e.g., systems programming personnel, operations staff, etc.).
-The PARMLIB authorization is restricted to only z/OS systems programming personnel and READ access may be given to auditors.
-The TESTAUTH authorization is restricted to only z/OS systems programming personnel.

Fix Text: Configure the TSOAUTH resource class to control sensitive TSO/E commands.

Note: The resource type, resources, and/or resource prefixes identified below are examples of a possible installation. The actual resource type, resources, and/or resource prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.

Below is listed the access requirements for TSOAUTH resources. Ensure the guidelines for the resources and/or generic equivalent are followed.

-The ACCT authorization is restricted to security personnel.
-The CONSOLE authorization is restricted to authorized systems personnel (e.g., systems programming personnel, operations staff, etc.) and READ access may be given to all user when SDSF in install at the ISSOs discretion.
-The MOUNT authorization is restricted to DASD batch users only.

-The OPER authorization is restricted to authorized systems personnel (e.g., systems programming personnel, operations staff, etc.).
-The PARMLIB authorization is restricted to only z/OS systems programming personnel and READ access may be given to audit users.
-The TESTAUTH authorization is restricted to only z/OS systems programming personnel.

CCI: CCI-000213

Group ID (Vulid): V-224073
Group Title: SRG-OS-000324-GPOS-00125
Rule ID: SV-224073r877911_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-TS-000020
Rule Title: CA-TSS LOGONIDs must not be defined to SYS1.UADS for non-emergency use.
Legacy ID: SV-107957
Legacy ID: V-98853

Vulnerability Discussion: Preventing non-privileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

Check Content:
Ask the system administrator to provide a list of all emergency userids available to the site along with the associated function of each.

If any SYS1.UADS userids are assigned for other than emergency purposes, this is a finding.

Fix Text: Configure the SYS1.UADS entries to ensure LOGONIDs defined include only those users required to support specific functions related to system recovery. Evaluate the impact of accomplishing the change.

CCI: CCI-002235

Group ID (Vulid): V-224074

Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-224074r877912_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000010
Rule Title: IBM z/OS UNIX HFS MapName file security parameters must be properly specified.
Legacy ID: SV-107959
Legacy ID: V-98855

Vulnerability Discussion: Removal of unneeded or non-secure functions, ports, protocols, and services mitigate the risk of unauthorized connection of devices, unauthorized transfer of information, or other exploitation of these resources.

Check Content:
Refer to the logical parmlib data sets, example: SYS1.PARMLIB(BPXPRMxx), for the following FILESYSTYPE entry:

FILESYSTYPE TYPE(AUTOMNT) ENTRYPOINT(BPXTAMD)

If the above entry is not found or is commented out in the BPXPRMxx member(s), this is not applicable.

From the ISPF Command Shell enter:
OMVS
cd /etc
cat auto.master
perform a contents list for the file identified
Example:
cat u.map
Note: The /etc/auto.master HFS file (and the use of Automount) is optional. If the file does not exist, this is not applicable.

Note: The setuid parameter and the security parameter have a significant security impact. For this reason these parameters must be explicitly specified and not allowed to default.

If each MapName file specifies the "setuid No" and "security Yes" statements for each automounted directory, this is not a finding.

If there is any deviation from the required values, this is a finding.

Fix Text: Review the settings in /etc/auto.master and /etc/mapname for z/OS UNIX security parameters and configure the values to conform to the specifications below.

The /etc/auto.master HFS file (and the use of Automount) is optional.

The setuid parameter and the security parameter have a significant security impact. For this reason these parameters must be explicitly specified and not be allowed to default.

Each MapName file will specify the "setuid NO" and "security YES" statements for each automounted directory.

If there is a deviation from the required values, documentation must exist for the deviation.

"Security NO" disables security checking for file access. "Security NO" is only allowed on test and development domains.

"Setuid YES" allows a user to run under a different UID/GID identity. Justification documentation is required to validate the use of "setuid YES".

CCI: CCI-000366

Group ID (Vulid): V-224075
Group Title: SRG-OS-000047-GPOS-00023
Rule ID: SV-224075r877913_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000020
Rule Title: IBM z/OS NOBUFFS in SMFPRMxx must be properly set (default is MSG).
Legacy ID: SV-107961
Legacy ID: V-98857

Vulnerability Discussion: It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Check Content:
Refer to IEASYS00 member in SYS1.PARMLIB Concatenation. Determine proper SMFPRMxx member in SYS1.PARMLIB.

If NOBUFFS is set to "HALT", this is not a finding.

Note: If availability is an overriding concern NOBUFFS can be set to MSG.

Fix Text: Configure NOBUFFS to "HALT" unless availability is an overriding concern then NOBUFFS can be set to MSG.

CCI: CCI-000140

Group ID (Vulid): V-224076
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224076r877914_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000030
Rule Title: IBM z/OS BPX resource(s) must be protected in accordance with security requirements.
Legacy ID: SV-107963
Legacy ID: V-98859

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
From the ISPF Command Shell enter:
TSS WHOOWNS IBMFAC(BPX.)

If the BPX. resource is properly owned, this is not a finding.

From the ISPF Command Shell enter:

TSS WHOHAS (<each BPX resource>)

If any item below are untrue, this is a finding.

-There are no TSS rules that allow access to the BPX resource.
-There are no TSS rules for BPX.SAFFASTPATH defined.
-The TSS rules for each of the BPX resources listed in the z/OS UNIX System Services Planning, Establishing UNIX security, restrict access to appropriate system tasks or systems programming personnel.

Fix Text: Because they convey especially powerful privileges, the settings for BPX.DAEMON, BPX.SAFFASTPATH, BPX.SERVER, and BPX.SUPERUSER require special attention.

Review the following items for the IBMFAC resource class:

-The TSS owner defined for the BPX resource.
-There are no TSS rules that allow access to the BPX resource.
-There are no TSS rules for BPX.SAFFASTPATH defined.

The TSS rules for each of the BPX resources listed in General Facility Class BPX Resources Table, in the z/OS UNIX System Services Planning, Establishing UNIX security restrict access to appropriate system tasks or systems programming personnel. Access can be permitted only to users with a requirement for the resource that is documented to the ISSO. Access to BPX.DAEMON must be restricted to the z/OS UNIX kernel userid, z/OS UNIX daemons (e.g., inetd, syslogd, ftpd), and other system software daemons (e.g., web servers). When BPX.SAFFASTPATH is defined, calls to the ACP are not performed for file accesses and there is no audit trail of access failures. This configuration is unacceptable. Therefore BPX.SAFFASTPATH must not be used on any system.

For Example:
The following commands can be used to provide the required protection:

TSS ADD(ADMIN) IBMFAC(BPX.)
TSS PERMIT(ALL) IBMFAC(BPX.SAFFASTPATH) ACCESS(NONE)

NOTE:
The PERMIT command for BPX.SAFFASTPATH must be executed on TOP SECRET systems. If access to BPX.SAFFSTPATH were allowed, z/OS UNIX would perform permission bit checking internally instead of calling the ACP. On TOP SECRET systems this would bypass any audit trail of violations. In addition, the z/OS UNIX kernel userid (OMVS is the example in this section) must not have the TOP SECRET NORESCHK privilege. Having that privilege would allow access to BPX.SAFFASTPATH even though the access restriction was in place.

CCI: CCI-000213

Group ID (Vulid): V-224077
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224077r877915_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000040
Rule Title: IBM z/OS UNIX resources must be protected in accordance with security requirements.
Legacy ID: V-98861
Legacy ID: SV-107965

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000326-GPOS-00126

Check Content:
From the ISPF Command Shell enter:
TSS WHOOWNS SURROGAT(*)

If the TSS resources and/or generic equivalent for BPX. is not owned enter:
TSS LIST RDT

If the TSS resources and/or generic equivalent for BPX. is not owned or DEFPROT is specified for the resource class, this is a finding.

From the ISPF Command Shell enter:
TSS WHOHAS SURROGAT(BPX.)

If the TSS resource access authorizations restrict BPX.SRV.user to system software processes

(e.g., web servers) that act as servers under z/OS UNIX, this is not a finding.

If the RACF rules for all BPX.SRV.user SURROGAT resources restrict access to authorized users identified in the Site Security Plan, this is not a finding.

Fix Text: Ensure that BPX. SRV.userid resources are properly protected and access is restricted to appropriate system tasks or systems programming personnel.

SURROGAT class BPX resources are used in conjunction with server applications that are performing tasks on behalf of client users that may not supply an authenticator to the server. This can be the case when clients are otherwise validated or when the requested service is performed from userids representing groups.

Ensure there is a TSS owner defined for the (BPX.) SURROGAT class resource.
For Example:
TSS ADD(dept) SURROGAT(BPX.)

Ensure the TSS rules for all BPX.SRV.user SURROGAT resources restrict access to system software processes (e.g., web servers) that act as servers under z/OS UNIX and to users whose access and approval are identified in the Site Security Plan.

For Example:
TSS PERMIT(<websrv>) SURROGAT(BPX.SRV.<webadm>)
ACCESS(READ)

CCI: CCI-000213

CCI: CCI-002233

Group ID (Vulid): V-224078
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224078r877916_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-US-000050
Rule Title: IBM z/OS UNIX SUPERUSER resources must be protected in accordance with guidelines.
Legacy ID: V-98863
Legacy ID: SV-107967

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information

by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
From the ISPF Command Shell enter:
TSS WHOOWNS UNIXPRIV(*)

If the TSS resources and/or generic equivalent for SUPERUSER. is not owned enter:
TSS LIST RDT

If the TSS resources and/or generic equivalent for SUPERUSER. is not owned or DEFPROT is specified for the resource class, this is a finding.

From the ISPF Command Shell enter:
TSS WHOHAS SURROGAT(SUPERUSER.)

If the TSS resource access authorizations restrict BPX.SRV.user to system software processes (e.g., web servers) that act as servers under z/OS UNIX, this is not a finding.

Fix Text: Ensure that all SUPERUSER resources for the UNIXPRIV resource class are restricted to appropriate system tasks and/or system programming personnel.

Review the following items for the UNIXPRIV resource class:

-The TSS owner defined for the SUPERUSER resource.
-There are no TSS rules that allow access to the SUPERUSER resource.
-There is no TSS rule for CHOWN.UNRESTRICTED defined.
-The TSS rules for each of the SUPERUSER resources listed in the z/OS UNIX System Services Planning, Establishing UNIX security, restrict access to appropriate system tasks or systems programming personnel.

CCI: CCI-000213

Group ID (Vulid): V-224079
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224079r877917_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000060
Rule Title: IBM z/OS UNIX MVS data sets or HFS objects must be properly protected.
Legacy ID: SV-107969
Legacy ID: V-98865

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100

Check Content:
Refer to the proper BPXPRMxx member in SYS1.PARMLIB

If the ESM data set rules for the data sets referenced in the ROOT and the MOUNT statements in BPXPRMxx restrict update access to the z/OS UNIX kernel (i.e., OMVS or OMVSKERN), this is not a finding.

If the ESM data set rules for the data set referenced in the ROOT and the MOUNT statements in BPXPRMxx restrict WRITE or greater access to systems programming personnel, this is not a finding.

Fix Text: Review the access authorizations defined in the ACP for the MVS data sets that contain operating system components and for the MVS data sets that contain HFS file systems and ensure that they conform to the specifications below.

Review the UNIX permission bits on the HFS directories and files and ensure that they conform to the specifications below:

Define ESM data set rules for the data sets referenced in the ROOT and the MOUNT statements in BPXPRMxx to restrict update access to the z/OS UNIX kernel (i.e., OMVS or OMVSKERN).

Define ESM data set rules for the data sets referenced in the ROOT and the MOUNT statements in BPXPRMxx to restrict WRITE or greater access to systems programming personnel.

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-224080
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224080r877918_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000070
Rule Title: IBM z/OS UNIX MVS data sets with z/OS UNIX components must be properly protected.
Legacy ID: SV-107971
Legacy ID: V-98867

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100

Check Content:
If the ESM data set rules for each of the data sets listed in the table below restrict WRITE or greater access to systems programming personnel, this is not a finding.

MVS DATA SETS WITH z/OS UNIX COMPONENTS
DATA SET NAME/MASK MAINTENANCE TYPE FUNCTION
SYS1.ABPX* Distribution IBM z/OS UNIX ISPF panels, messages, tables, clists
SYS1.AFOM* Distribution IBM z/OS UNIX Application Services
SYS1.BPA.ABPA* Distribution IBM z/OS UNIX Connection Scaling Process Mgr.
SYS1.CMX.ACMX* Distribution IBM z/OS UNIX Connection Scaling Connection Mgr.
SYS1.SBPX* Target IBM z/OS UNIX ISPF panels, messages, tables, clists
SYS1.SFOM* Target IBM z/OS UNIX Application Services
SYS1.CMX.SCMX* Target IBM z/OS UNIX Connection Scaling Connection Mgr.

Fix Text: Define ESM data set rules for each of the data sets listed in the table below; restrict WRITE or greater access to systems programming personnel.

MVS DATA SETS WITH z/OS UNIX COMPONENTS
DATA SET NAME/MASK MAINTENANCE TYPE FUNCTION
SYS1.ABPX* Distribution IBM z/OS UNIX ISPF panels, messages, tables, clists
SYS1.AFOM* Distribution IBM z/OS UNIX Application Services
SYS1.BPA.ABPA* Distribution IBM z/OS UNIX Connection Scaling Process Mgr.
SYS1.CMX.ACMX* Distribution IBM z/OS UNIX Connection Scaling Connection Mgr.
SYS1.SBPX* Target IBM z/OS UNIX ISPF panels, messages, tables, clists
SYS1.SFOM* Target IBM z/OS UNIX Application Services
SYS1.CMX.SCMX* Target IBM z/OS UNIX Connection Scaling Connection Mgr.

The data sets designated as distribution data sets should have all access restricted to systems programming personnel. TSO/E users who also use z/OS UNIX should have read access to the SYS1.SBPX* data sets. Read access for all users to the remaining target data sets is at the site's discretion. All other access must be restricted to systems programming personnel.

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-224081
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224081r877919_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000080
Rule Title: IBM z/OS UNIX MVS data sets used as step libraries in /etc/steplib must be properly protected.

Legacy ID: SV-107973
Legacy ID: V-98869

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100, SRG-OS-000324-GPOS-00125

Check Content:
Refer to the pathname from the STEPLIBLIST line in BPXPRMxx member of PARMLIB.
From the ISPF Command shell enter:
ISHELL

on the command line:
on the path name line enter:
/etc/

From the resulting display scroll down to the <stepliblist name> from BPXPRMxx parm.

Enter B for browse on that line.

If ESM data set rules for libraries specified restrict WRITE or greater access to only systems programming personnel, this is not a finding.

If the ESM data set rules for libraries specify that all (i.e., failures and successes) WRITE or greater access will be logged, this is not a finding.

Fix Text: Configure the WRITE or greater access to libraries residing in the /etc/steplib to be limited to system programmers only.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-224082
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224082r877920_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000090
Rule Title: IBM z/OS UNIX HFS permission bits and audit bits for each directory must be properly protected.
Legacy ID: SV-107975
Legacy ID: V-98871

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100

Check Content:
From the ISPF Command Shell enter:
omvs

enter CD /

enter ls -alW

If the HFS permission bits and user audit bits for each directory and file match or are more restrictive than the specified settings listed in the SYSTEM DIRECTORY SECURITY SETTINGS table below, this is not a finding.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
- no auditing

SYSTEM DIRECTORY SECURITY SETTINGS
DIRECTORY PERMISSION BITS USER AUDIT BITS FUNCTION
/ [root] 755 faf Root level of all file systems. Holds critical mount points.
/bin 1755 fff Shell scripts and executables for basic functions
/dev 1755 fff Character-special files used when logging into the OMVS shell and during C language program compilation.
Files are created during system IPL and on a per-demand basis.
/etc 1755 faf Configuration programs and files (usually with locally customized data) used by z/OS UNIX and other product initialization processes
/lib 1755 fff System libraries including dynamic link libraries and files for static linking
/samples 1755 fff Sample configuration and other files
/tmp 1777 fff Temporary data used by daemons, servers, and users. Note: /tmp must have the sticky bit on to restrict file renames and deletions.
/u 1755 fff Mount point for user home directories and optionally for third-party software and other local site files
/usr 1755 fff Shell scripts, executables, help (man) files and other data. Contains sub-directories (e.g., lpp) and mount points used by program products that may be in separate file systems.
/var 1775 fff Dynamic data used internally by products and by elements and features of z/OS UNIX.

Fix Text: Configure the UNIX permission bits and user audit bits on each of the HFS directories in the table SYSTEM DIRECTORY SECURITY SETTINGS below to be equal or more restrictive.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
- no auditing

SYSTEM DIRECTORY SECURITY SETTINGS
DIRECTORY PERMISSION BITS USER AUDIT BITS FUNCTION
/ [root] 755 faf Root level of all file systems. Holds critical mount points.
/bin 1755 fff Shell scripts and executables for basic functions
/dev 1755 fff Character-special files used when logging into the OMVS shell and during C language program compilation.
Files are created during system IPL and on a per-demand basis.
/etc 1755 faf Configuration programs and files (usually with locally customized data) used by z/OS UNIX and other product initialization processes
/lib 1755 fff System libraries including dynamic link libraries and files for static linking
/samples 1755 fff Sample configuration and other files
/tmp 1777 fff Temporary data used by daemons, servers, and users. Note: /tmp must have the sticky bit on to restrict file renames and deletions.
/u 1755 fff Mount point for user home directories and optionally for third-party software and other local site files
/usr 1755 fff Shell scripts, executables, help (man) files and other data. Contains sub-directories (e.g., lpp) and mount points used by program products that may be in separate file systems.
/var 1775 fff Dynamic data used internally by products and by elements and features of z/OS UNIX.

The following commands are a sample of the commands to be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

chmod 0755 /
chaudit w=sf,rx+f /
chmod 0755 /bin
chaudit rwx=f /bin

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-224083
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224083r877921_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000100
Rule Title: IBM z/OS UNIX system file security settings must be properly protected or specified.
Legacy ID: SV-107977
Legacy ID: V-98873

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100

Check Content:
From the ISPF Command Shell enter:
OMVS
For each file listed in the table below enter:
ls -alW /<directory name>/<file name>

If the HFS permission bits and user audit bits for each directory and file match or are more restrictive than the specified settings listed in the table, this is not a finding.

NOTE: Some of the files listed are not used in every configuration. Absence of any of the files is not considered a finding.

SYSTEM FILE SECURITY SETTINGS
FILE PERMISSION BITS USER AUDIT BITS FUNCTION
/bin/sh 1755 faf z/OS UNIX shell
Note: /bin/sh has the sticky bit on to improve performance.
/dev/console 740 fff The system console file receives messages that may require System Administrator (SA) attention.
/dev/null 666 fff A null file; data written to it is discarded.
/etc/auto.master
any mapname files 740 faf Configuration files for automount facility
/etc/inetd.conf 740 faf Configuration file for network services
/etc/init.options 740 faf Kernel initialization options file for z/OS UNIX environment
/etc/log 744 fff Kernel initialization output file
/etc/profile 755 faf Environment setup script executed for each user
/etc/rc 744 faf Kernel initialization script for z/OS UNIX environment
/etc/steplib 740 faf List of MVS data sets valid for set user ID and set group ID executables
/etc/table name 740 faf List of z/OS userids and group names with corresponding alias names
/usr/lib/cron/at.allow
/usr/lib/cron/at.deny 700 faf Configuration files for the at and batch commands
/usr/lib/cron/cron.allow
/usr/lib/cron/cron.deny 700 faf Configuration files for the crontab command

NOTE: Some of the files listed are not used in every configuration. Absence of any of the files is not considered a finding.

NOTE: The names of the MapName files are site-defined. Refer to the listing in the EAUTOM report.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
- no auditing

Fix Text: Define the UNIX permission bits and user audit bits on the HFS files as listed in the table below.

SYSTEM FILE SECURITY SETTINGS
FILE PERMISSION BITS USER AUDIT BITS FUNCTION
/bin/sh 1755 faf z/OS UNIX shell
Note: /bin/sh has the sticky bit on to improve performance.
/dev/console 740 fff The system console file receives messages that may require System Administrator (SA) attention.
/dev/null 666 fff A null file; data written to it is discarded.
/etc/auto.master
any mapname files 740 faf Configuration files for automount facility
/etc/inetd.conf 740 faf Configuration file for network services
/etc/init.options 740 faf Kernel initialization options file for z/OS UNIX environment
/etc/log 744 fff Kernel initialization output file
/etc/profile 755 faf Environment setup script executed for each user
/etc/rc 744 faf Kernel initialization script for z/OS UNIX environment
/etc/steplib 740 faf List of MVS data sets valid for set user ID and set group ID executables
/etc/table name 740 faf List of z/OS userids and group names with corresponding alias names
/usr/lib/cron/at.allow
/usr/lib/cron/at.deny 700 faf Configuration files for the at and batch commands
/usr/lib/cron/cron.allow
/usr/lib/cron/cron.deny 700 faf Configuration files for the crontab command

There are a number of files that must be secured to protect system functions in z/OS UNIX. Where not otherwise specified, these files must receive a permission setting of 744 or 774. The 774 setting may be used at the site's discretion to help to reduce the need for assignment of superuser privileges. The table identifies permission bit and audit bit settings that are required for these specific files. More restrictive permission settings may be used at the site's discretion or as specific environments dictate.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts

a log for failed and successful access
- no auditing

The following commands are a sample of the commands to be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

chmod 1755 /bin/sh
chaudit w=sf,rx+f /bin/sh
chmod 0740 /dev/console
chaudit rwx=f /dev/console

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-224084
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224084r877922_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000110
Rule Title: IBM z/OS UNIX MVS HFS directory(s) with OTHER write permission bit set must be properly defined.
Legacy ID: V-98875
Legacy ID: SV-107979

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
On the OMVS Command line enter the following command string:
find / -type d -perm -0002 ! -perm -1000 -exec ls -aldWE {} \;

If there are no directories that have the other write permission bit set on without the sticky bit set on, there is no finding.

NOTE: In the symbolic permission bit display, the sticky bit is indicated as a "t" or "T" in the execute portion of the other permissions. For example, a display of the permissions of a directory with the sticky bit on could be "drwxrwxrwt".

If all directories that have the other write permission bit set on do not contain any files with the setuid bit set on, this is not a finding.

NOTE: In the symbolic permission bit display, the setuid bit is indicated as an "s" or "S" in the execute portion of the owner permissions. For example, a display of the permissions of a file with the setuid bit on could be "-rwsrwxrwx".

If all directories that have the other write permission bit set on do not contain any files with the setgid bit set on, this is not a finding.

NOTE: In the symbolic permission bit display, the setgid bit is indicated as an "s" or "S" in the execute portion of the group permissions. For example, a display of the permissions of a file with the setgid bit on could be "-rwxrwsrwx".

Fix Text: Configure directory permissions as follows
There are no directories that have the other write permission bit set on without the sticky bit set on.

NOTE: In the symbolic permission bit display, the sticky bit is indicated as a "t" or "T" in the execute portion of the other permissions. For example, a display of the permissions of a directory with the sticky bit on could be "drwxrwxrwt".

All directories that have the other write permission bit set on do not contain any files with the setuid bit set on.

NOTE: In the symbolic permission bit display, the setuid bit is indicated as an "s" or "S" in the execute portion of the owner permissions. For example, a display of the permissions of a file with the setuid bit on could be "-rwsrwxrwx".

All directories that have the other write permission bit set on do not contain any files with the setgid bit set on.

NOTE: In the symbolic permission bit display, the setgid bit is indicated as an "s" or "S" in the execute portion of the group permissions. For example, a display of the permissions of a file with the setgid bit on could be "-rwxrwsrwx".

CCI: CCI-000213

Group ID (Vulid): V-224085
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224085r877923_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-US-000120
Rule Title: The CA-TSS HFSSEC resource class must be defined with DEFPROT.
Legacy ID: V-98877
Legacy ID: SV-107981

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
From the ISPF Command Shell enter:
TSS MODIFY STATUS
If the Control Option is HFSSEC(OFF), this is Not Applicable.

Enter:
TSS LIST RDT
If the DEFPROT attribute is specified for the HFSSEC resource class in the RDT, this is not a finding.

Fix Text: Ensure that the HFSSEC resource class has the attribute DEFPROT.

For Example:

TSS REPLACE(RDT) RESCLASS(HFSSEC) ATTR(DEFPROT)

CCI: CCI-000213

Group ID (Vulid): V-224086
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-224086r877924_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000130
Rule Title: IBM z/OS UNIX OMVS parameters in PARMLIB must be properly specified.
Legacy ID: V-98879
Legacy ID: SV-107983

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Check Content:
Refer to the IEASYS00 member of SYS1.PARMLIB.
If the parameter is specified as OMVS=xx or OMVS=(xx,xx,...) in the IEASYSxx member, this is not a finding.

If the OMVS statement is not specified, OMVS=DEFAULT is used. In minimum mode there is no access to permanent file systems or to the shell, and IBM's Communication Server TCP/IP will not run.

Fix Text: Configure the settings in PARMLIB and /etc for z/OS UNIX security parameters with values that conform to the specifications below:

The parameter is specified as OMVS=xx or OMVS=(xx,xx,...) in the IEASYSxx member.

Note: If the OMVS statement is not specified, OMVS=DEFAULT is used. In minimum mode there is no access to permanent file systems or to the shell, and IBM's Communication Server

TCP/IP will not run.

CCI: CCI-000366

Group ID (Vulid): V-224087
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-224087r877925_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000140
Rule Title: IBM z/OS UNIX BPXPRMxx security parameters in PARMLIB must be properly specified.
Legacy ID: V-98881
Legacy ID: SV-107985

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Check Content:
Refer to the BPXPRM00 member of SYS1.PARMLIB.
If the required parameter keywords and values are defined as detailed below, this is not a finding.

Parameter Keyword Value
SUPERUSER BPXROOT
TTYGROUP TTY
STEPLIBLIST /etc/steplib
USERIDALIASTABLE Will not be specified.
ROOT SETUID will be specified
MOUNT NOSETUID
SETUID (for Vendor-provided files)SECURITY
STARTUP_PROC OMVS

Fix Text: Define the settings in PARMLIB member BPXPRMxx for z/OS UNIX security parameters values to conform to the specifications below:
Parameter Keyword Value
SUPERUSER BPXROOT
TTYGROUP TTY
STEPLIBLIST /etc/steplib
USERIDALIASTABLE Will not be specified.
ROOT SETUID will be specified
MOUNT NOSETUIDSETUID (for Vendor-provided files)SECURITY

STARTUP_PROC OMVS

CCI: CCI-000366

Group ID (Vulid): V-224088
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224088r877926_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000150
Rule Title: IBM z/OS UNIX security parameters in etc/profile must be properly specified.
Legacy ID: V-98883
Legacy ID: SV-107987

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Check Content:
From the ISPF Command Shell enter:
ISHELL
/etc/profile
If the final or only instance of the UMASK command in /etc/profile is specified as "umask 077", this is not a finding.

If the LOGNAME variable is marked read-only (i.e., "readonly LOGNAME") in /etc/profile, this is not a finding.

Fix Text: Configure the etc/profile to specify the UMASK command is executed with a value of 077 and the LOGNAME variable is marked read-only for the /etc/profile file, exceptions are documented with the ISSO.

CCI: CCI-000213

Group ID (Vulid): V-224089
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224089r877927_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000160
Rule Title: IBM z/OS UNIX security parameters in /etc/rc must be properly specified.

Legacy ID: V-98885
Legacy ID: SV-107989

Vulnerability Discussion: Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Check Content:
From the ISPF Command Shell enter:
ISHELL
/etc/rc

If all of the CHMOD commands in /etc/rc do not result in less restrictive access than what is specified in the tables below, this is not a finding.

NOTE: The use of CHMOD commands in /etc/rc is required in most environments to comply with the required settings, especially for dynamic objects such as the /dev directory.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

If all of the CHAUDIT commands in /etc/rc do not result in less auditing than what is specified in the tables below, this is not a finding.

NOTE: The use of CHAUDIT commands in /etc/rc may not be necessary. If none are found, there is not a finding.

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
- no auditing

If the _BPX_JOBNAME variable is appropriately set (i.e., to match daemon name) as each daemon (e.g., syslogd, inetd) is started in /etc/rc, this is not a finding.

NOTE: If _BPX_JOBNAME is not specified, the started address space will be named using an inherited value. This could result in reduced security in terms of operator command access.

SYSTEM DIRECTORY SECURITY SETTINGS
DIRECTORY PERMISSION BITS USER AUDIT BITS FUNCTION
/ [root] 755 faf Root level of all file systems. Holds critical mount points.
/bin 1755 fff Shell scripts and executables for basic functions
/dev 1755 fff Character-special files used when logging into the OMVS shell and during C language program compilation.
Files are created during system IPL and on a per-demand basis.
/etc 1755 faf Configuration programs and files (usually with locally customized data) used by z/OS UNIX and other product initialization processes
/lib 1755 fff System libraries including dynamic link libraries and files for static linking
/samples 1755 fff Sample configuration and other files
/tmp 1777 fff Temporary data used by daemons, servers, and users. Note: /tmp must have the sticky bit on to restrict file renames and deletions.
/u 1755 fff Mount point for user home directories and optionally for third-party software and other local site files
/usr 1755 fff Shell scripts, executables, help (man) files and other data. Contains sub-directories (e.g., lpp) and mount points used by program products that may be in separate file systems.
/var 1775 fff Dynamic data used internally by products and by elements and features of z/OS UNIX.

SYSTEM FILE SECURITY SETTINGS
FILE PERMISSION BITS USER AUDIT BITS FUNCTION
/bin/sh 1755 faf z/OS UNIX shell
Note: /bin/sh has the sticky bit on to improve performance.
/dev/console 740 fff The system console file receives messages that may require System Administrator (SA) attention.
/dev/null 666 fff A null file; data written to it is discarded.
/etc/auto.master and
any mapname files 740 faf Configuration files for automount facility
/etc/inetd.conf 740 faf Configuration file for network services
/etc/init.options 740 faf Kernel initialization options file for z/OS UNIX environment
/etc/log 744 fff Kernel initialization output file
/etc/profile 755 faf Environment setup script executed for each user
/etc/rc 744 faf Kernel initialization script for z/OS UNIX environment
/etc/steplib 740 faf List of MVS data sets valid for set user ID and set group ID executables
/etc/table name 740 faf List of z/OS userids and group names with corresponding alias names
/usr/lib/cron/at.allow
/usr/lib/cron/at.deny 700 faf Configuration files for the at and batch commands
/usr/lib/cron/cron.allow

/usr/lib/cron/cron.deny 700 faf Configuration files for the crontab command

Fix Text: Review the settings in the /etc/rc. The /etc/rcfile is the system initialization shell script. When z/OS UNIX kernel services start, /etc/rc is executed to set file permissions and ownership for dynamic system files and to perform other system startup functions such as starting daemons. There can be many commands in /etc/rc. There are two specific guidelines that must be followed:

Verify that The CHMOD or CHAUDIT command does not result in less restrictive security than what is specified in the table in the z/OS UNIX System Services Planning, Establishing UNIX security under the SYSTEM DIRECTORY SECURITY SETTINGS.

Immediately prior to each command that starts a daemon, the _BPX_JOBNAME variable must be set to match the daemon's name (e.g., inetd, syslogd). The use of _BPX_USERID is at the site's discretion, but is recommended.

CCI: CCI-000213

Group ID (Vulid): V-224090
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-224090r877928_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000170
Rule Title: IBM z/OS Default profiles must not be defined in TSS OMVS UNIX security parameters for classified systems.
Legacy ID: V-98887
Legacy ID: SV-107991

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Check Content:
If the system in not classified this is not applicable.

From a command line issue the following command:
TSS MODIFY STATUS
Note: One must have appropriate access to perform this command (have the site security officer to issue command).

If system is classified and UNIQUSER is off i.e., (UNIQUSER(OFF) this is not a finding.

Fix Text: Ensure that Use of the OMVS default UIDs will not be allowed on any classified system.

Set Control Option UNIQUSER off.

CCI: CCI-000366

Group ID (Vulid): V-224091
Group Title: SRG-OS-000096-GPOS-00050
Rule ID: SV-224091r877929_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000180
Rule Title: IBM z/OS UNIX security parameters for restricted network service(s) in /etc/inetd.conf must be properly specified.
Legacy ID: V-98889
Legacy ID: SV-107993

Vulnerability Discussion: In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., VPN and IPS); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the operating system must support the organizational requirements, providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

Check Content:
From the UNIX System Services ISPF Shell enter
/etc/inetd.conf

If any Restricted Network Services that are listed below are specified or not commented out this is a finding.

RESTRICTED NETWORK SERVICES/PORTS
Service Port

Chargen 19
Daytime 13
Discard 9
Echo 7
Exec 512
finger 79
shell 514
time 37
login 513
smtp 25
timed 525
nameserver 42
systat 11
uucp 540
netstat 15
talk 517
qotd 17
tftp 69

Fix Text: Review the settings in The /etc/inetd.conf file determine if every entry in the file represents a service that is actually in use. Services that are not in use must be disabled to reduce potential security exposures.

The following services must be disabled in /etc/inetd.conf unless justified and documented with the ISSO:

RESTRICTED NETWORK SERVICES

Service Port
Chargen 19
Daytime 13
Discard 9
Echo 7
Exec 512
finger 79
shell 514
time 37
login 513
smtp 25
timed 525
nameserver 42
systat 11
uucp 540
netstat 15
talk 517
qotd 17

tftp 69

/etc/inetd.conf

The /etc/inetd.conf file is used by the INETD daemon. It specifies how INETD is to handle service requests on network sockets. Specifically, there is one entry in inetd.conf for each service. Each service entry specifies several parameters. The login_name parameter is of special interest. It specifies the userid under which the forked daemon is to execute. This userid is defined to the ACP and it may require a UID(0) (i.e., superuser authority) value.

CCI: CCI-000382

Group ID (Vulid): V-224092
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-224092r877930_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000190
Rule Title: IBM z/OS attributes of z/OS UNIX user accounts must have a unique GID in the range of 1-99.
Legacy ID: SV-107995
Legacy ID: V-98891

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
A site can choose to have both an OMVSGRP group and an STCOMVS group or combine the groups under one of these names.

If OMVSGRP and/or STCOMVS groups are defined and have a unique GID in the range of 1-99, this is not a finding.

Fix Text: Define the OMVSGRP group and/or the STCOMVS group to the security database with a unique GID in the range of 1-99.

OMVSGRP is the name suggested by IBM for all the required userids. STCOMVS is the standard name used at some sites for the userids that are associated with z/OS UNIX started tasks and daemons. These groups can be combined at the site's discretion.

CCI: CCI-000764

Group ID (Vulid): V-224093
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-224093r877931_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000200
Rule Title: The IBM z/OS user account for the UNIX kernel (OMVS) must be properly defined to the security database.
Legacy ID: SV-107997
Legacy ID: V-98893

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
If OMVS userid is defined to the ESM as follows, this is not a finding.

-No access to interactive on-line facilities (e.g., TSO, CICS, etc.)
-Default group specified as OMVSGRP or STCOMVS
-UID(0)
-HOME directory specified as "/"
-Shell program specified as "/bin/sh"

Fix Text: Define OMVS userid to the ESM as specified below:

-No access to interactive on-line facilities (e.g., TSO, CICS, etc.)
-Default group specified as OMVSGRP or STCOMVS
-UID(0)
-HOME directory specified as "/"
-Shell program specified as "/bin/sh"

CCI: CCI-000764

Group ID (Vulid): V-224094
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-224094r877932_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000210
Rule Title: The IBM z/OS user account for the z/OS UNIX SUPERUSER userid must be properly defined.
Legacy ID: SV-107999
Legacy ID: V-98895

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
Refer to system PARMLIB member BPXPRMxx (xx is determined by OMVS entry in IEASYS00.)

Determine the user ID identified by the SUPERUSER parameter. (BPXROOT is the default).

From a command input screen enter:
LISTUSER (superuser userid) TSO CICS OMVS

If the SUPERUSER userid is defined as follows, this is not a finding:

- No access to interactive on-line facilities (e.g., TSO, CICS, etc.)
- Default group specified as OMVSGRP or STCOMVS
- UID(0)
- HOME directory specified as "/"
- Shell program specified as "/bin/sh"

Fix Text: Define the user ID identified in the BPXPRM00 SUPERUSER parameter as specified below:

- No access to interactive on-line facilities (e.g., TSO, CICS, etc.)
- Default group specified as OMVSGRP or STCOMVS
- UID(0)
- HOME directory specified as "/"
- Shell program specified as "/bin/sh"

CCI: CCI-000764

Group ID (Vulid): V-224095
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-224095r877933_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000220
Rule Title: The IBM z/OS user account for the UNIX (RMFGAT) must be properly defined.
Legacy ID: SV-108001
Legacy ID: V-98897

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
RMFGAT is the userid for the Resource Measurement Facility (RMF) Monitor III Gatherer. If RMFGAT is not define this is not applicable.

From a command input screen enter:

TSS LIST (RMFGAT) DATA ALL

If RMFGAT is defined as follows, this is not a finding:

-Default group specified as OMVSGRP or STCOMVS
-A unique, non-zero UID
-HOME directory specified as "/"
-Shell program specified as "/bin/sh"

Fix Text: Define RMFGAT user account is defined as specified below:

-Default group specified as OMVSGRP or STCOMVS
-A unique, non-zero UID
-HOME directory specified as "/"
-Shell program specified as "/bin/sh"

CCI: CCI-000764

Group ID (Vulid): V-224096
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-224096r877934_rule
Severity: CAT I
Rule Version (STIG-ID): TSS0-US-000230
Rule Title: IBM z/OS UID(0) must be properly assigned.

Legacy ID: SV-108003
Legacy ID: V-98899

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
From the ISPF Command Shell enter:
TSS LIST(ACIDS) SEGMENT(OMVS)

If UID(0) is assigned only to system tasks such as the z/OS/ UNIX kernel (i.e., OMVS), z/OS UNIX daemons (e.g., inetd, syslogd, ftpd), and other system software daemons, this is not a finding.

If UID(0) is assigned to security administrators who create or maintain user account definitions; and to systems programming accounts dedicated to maintenance (e.g., SMP/E) of HFS-based components, this is not a finding.

NOTE: The assignment of UID(0) confers full time superuser privileges. This is not appropriate for personal user accounts. Access to the BPX.SUPERUSER resource is used to allow personal user accounts to gain short-term access to superuser privileges.

If UID(0) is assigned to non-systems or non-maintenance accounts, this is a finding.

Fix Text: Ensure that UID(0) is defined/assigned as specified below:
UID(0) is assigned only to system tasks such as the z/OS UNIX kernel (i.e., OMVS), z/OS UNIX daemons (e.g., inetd, syslogd, ftpd), and other system software daemons.

UID(0) is assigned to security administrators who create or maintain user account definitions; and to systems programming accounts dedicated to maintenance (e.g., SMP/E) of HFS-based

components.

NOTE: The assignment of UID(0) confers full time superuser privileges, this is not appropriate for personal user accounts. Access to the BPX.SUPERUSER resource is used to allow personal user accounts to gain short-term access to superuser privileges.

CCI: CCI-000764

Group ID (Vulid): V-224097
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-224097r877935_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000240
Rule Title: IBM z/OS UNIX user accounts must be properly defined.
Legacy ID: SV-108005
Legacy ID: V-98901

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
NOTE: This only applies to users of z/OS UNIX (i.e., users with an OMVS profile defined).

From the ISPF Command Shell enter:
TSS LIST(ACIDS) SEGMENT(OMVS)

If any user account is not defined as follows, this is a finding.

-A unique UID number (except for UID(0) users)
-A unique HOME directory (except for UID(0) and other system task accounts)
-Shell program specified as "/bin/sh", "/bin/tcsh", "/bin/echo", or "/bin/false"

NOTE: The shell program must have one of the specified values. The HOME directory must have a value (i.e., not be allowed to default).

Fix Text: Configure each user account to be defined as specified below:

NOTE: This only applies to users of z/OS UNIX (i.e., users with an OMVS profile defined).

-A unique UID number (except for UID(0) users)
-A unique HOME directory (except for UID(0) and other system task accounts)
-Shell program specified as "/bin/sh", "/bin/tcsh", "/bin/echo", or "/bin/false"

NOTE: The shell program must have one of the specified values. The HOME directory must have a value (i.e., not be allowed to default).

CCI: CCI-000764

Group ID (Vulid): V-224098
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-224098r877936_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-US-000250
Rule Title: IBM z/OS attributes of UNIX user accounts used for account modeling must be defined in accordance with security requirements.
Legacy ID: SV-108007
Legacy ID: V-98903

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:
From the ISPF Command Shell enter:
TSS LIST(ACIDS) DATA(NAME) SEGMENT(OMVS)
This check applies to any user identifier (ACID) used to model OMVS access on the mainframe. This includes OMVSUSR; MODLUSER, and BPX.UNIQUE.USER.
ENTER
TSS MODIFY STATUS

If ANY MODLUSER is specified then UNIQUSER must be specified as "ON" in the STATUS.

If user identifier (ACID) used to model OMVS user account is defined as follows, this is not finding.

A non-writable HOME directory
Shell program specified as "/bin/echo", or "/bin/false"

Note: The shell program must have one of the specified values. The HOME directory must have a value (i.e., not be allowed to default).

Fix Text: Use of the OMVS default UID will not be allowed on any classified system.

Define the user identifier (ACID) used to model OMVS user account with a non-writable home directory, such as "\" root, and a non-executable, but existing, binary file, "/bin/false" or "/bin/echo."

CCI: CCI-000764

Group ID (Vulid): V-224099
Group Title: SRG-OS-000024-GPOS-00007
Rule ID: SV-224099r877939_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-UT-000010
Rule Title: The IBM z/OS UNIX Telnet server etc/banner file must have the Standard Mandatory DoD Notice and Consent Banner.
Legacy ID: SV-108009
Legacy ID: V-98905

Vulnerability Discussion: Display of a standardized and approved use notification before

granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read & consent to terms in IS user agreem't."

Satisfies: SRG-OS-000024-GPOS-00007, SRG-OS-000023-GPOS-00006

Check Content:
From UNIX System Services ISPF Shell, enter path "/etc/otelnet/banner/".
If this file does not contain the banner below, check the UNIX System Services ISPF Shell path

/etc/banner.
If neither file contains the banner below, this is a finding.
If the banner below is contained in either, this is not a finding.

This banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Fix Text: Configure the /etc/otelnet/banner file and ensure the text specifies a logon banner in accordance with DISA requirements.

Alternately, the /etc/banner file may be used in accordance with DISA requirements.

CCI: CCI-000048

CCI: CCI-000050

Group ID (Vulid): V-224100
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224100r877940_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-UT-000020
Rule Title: The IBM z/OS startup user account for the z/OS UNIX Telnet server must be properly defined.
Legacy ID: SV-108011
Legacy ID: V-98907

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Check Content:
From the ISPF Command Shell enter:
omvs
cd /etc
cat inetd.conf

If the "otelnetd" command specifies any user other than "OMVS" or "OMVSKERN", this is a finding.

Fix Text: The user account used at the startup of "otelnetd" is specified in the "inetd" configuration file. This account is used to perform the identification and authentication of the user requesting the session. Because the account is only used until user authentication is completed, there is no need for a unique account for this function. The z/OS UNIX kernel

account can be used.

CCI: CCI-000213

Group ID (Vulid): V-224101
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224101r877941_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-UT-000030
Rule Title: IBM z/OS HFS objects for the z/OS UNIX Telnet server must be properly protected.
Legacy ID: SV-108013
Legacy ID: V-98909

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100

Check Content:
From the ISPF Command Shell enter:
omvs

At the input line enter:
cd /usr
enter
ls -alW

If the following File permission and user Audit Bits are true, this is not a finding.

/usr/sbin/otelnetd 1740 fff

cd /etc
ls -alW
If the following file permission and user Audit Bits are true this is not a finding.
/etc/banner 0744 faf

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
- no auditing

Fix Text: With the assistance of a systems programmer with UID(0) and/or SUPERUSER access, will review the UNIX permission bits and user audit bits on the HFS directories and files for the z/OS UNIX Telnet Server. Ensure they conform to the specifications below:

z/OS UNIX TELNET Server HFS Object Security Settings
File Permission Bits User Audit Bits
/usr/sbin/otelnetd 1740 fff
/etc/banner 0744 faf

NOTE: The /usr/sbin/otelnetd object is a symbolic link to /usr/lpp/tcpip/sbin/otelnetd. The permission and user audit bits on the target of the symbolic link must have the required settings.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
- no auditing

The following commands can be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

chmod 1740 /usr/lpp/tcpip/sbin/otelnetd
chaudit rwx=f /usr/lpp/tcpip/sbin/otelnetd
chmod 0744 /etc/banner
chaudit w=sf,rx+f /etc/banner

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-224102
Group Title: SRG-OS-000228-GPOS-00088
Rule ID: SV-224102r877942_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-UT-000040
Rule Title: The IBM z/OS UNIX Telnet server Startup parameters must be properly specified.
Legacy ID: V-98911
Legacy ID: SV-108015

Vulnerability Discussion: Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

Check Content:
From the ISPF Command Shell enter:
ISHELL

Enter /etc/ for a pathname - you may need to issue a CD /etc/

select FILE NAME inetd.conf

If Option -D login is included on the otelnetd command, this is not a finding.

If Option -c 900 is included on the otelnetd command, this is not a finding.

NOTE: "900" indicates a session timeout value of "15" minutes and is currently the maximum value allowed.

Fix Text: Configure the startup parameters in the inetd.conf file for otelnetd to conform to the specifications below.

The otelnetd startup command includes the options -D login and -c 900, where:

-D login indicates that messages should be written to the syslogd facility for login and logout activity.

-c 900 indicates that the Telnet session should be terminated after "15" minutes of inactivity.

NOTE: "900" is the maximum value; any value between "1" and "900" is acceptable.

CCI: CCI-000366

Group ID (Vulid): V-224103
Group Title: SRG-OS-000228-GPOS-00088
Rule ID: SV-224103r877943_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-UT-000050
Rule Title: The IBM z/OS UNIX Telnet server warning banner must be properly specified.
Legacy ID: V-98913
Legacy ID: SV-108017

Vulnerability Discussion: Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

Check Content:
From the ISPF Command Shell enter:

OMVS
cat inetd.conf

If the otelnet startup command includes option "-h" this is a finding.

Fix Text: The otelnetd startup command should not include the option "-h", where:

-h indicates that the logon banner should not be displayed.

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

Group ID (Vulid): V-224104
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-224104r877944_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-VT-000010
Rule Title: IBM z/OS System data sets used to support the VTAM network must be properly secured.
Legacy ID: SV-108019
Legacy ID: V-98915

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100

Check Content:
Create a list of data set names containing all VTAM start options, configuration lists, network resource definitions, commands, procedures, exit routines, all SMP/E TLIBs, and all SMP/E DLIBs used for installation and in development/production VTAM environments.
If the ESM data set rules for all VTAM system data sets restrict access to only network systems programming staff, this is not a finding.
If RACF data set rules for all VTAM system data sets all READ access to auditors only, this is not a finding.

These data sets include libraries containing VTAM load modules and exit routines, and VTAM start options and definition statements.

Fix Text: Configure TSS data set rules for all VTAM system data sets restrict access to only network systems programming staff.
Auditors may have READ access as documented by and approved by the ISSM.

These data sets include libraries containing VTAM load modules and exit routines, and VTAM start options and definition statements.

The following sample TSS commands show proper permissions for VTAM data sets (replace "profile" with the profile name of the network systems programming staff authorities):

TSS PERMIT(profile) DSN(SYS1.VTAM.) ACC(ALL)
TSS PERMIT(profile) DSN('SYS1.VTAMLIB.) ACC(ALL)
TSS PERMIT(profile) DSN(SYS1.VTAM.SISTCLIB.) ACC(ALL)
TSS PERMIT(profile) DSN(SYS3.VTAM.) ACC(ALL)
TSS PERMIT(profile) DSN(SYS3.VTAMLIB.) ACC(ALL)

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-224105
Group Title: SRG-OS-000259-GPOS-00100

Rule ID: SV-224105r877945_rule
Severity: CAT II
Rule Version (STIG-ID): TSS0-VT-000020
Rule Title: IBM z/OS VTAM USSTAB definitions must not be used for unsecured terminals.
Legacy ID: SV-108021
Legacy ID: V-98917

Vulnerability Discussion: If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Check Content:
Ask the system administrator to supply the following information:

- Documentation regarding terminal naming standards.
- Documentation of all procedures controlling terminal logons to the system.
- A complete list of all USS commands used by terminal users to log on to the system.
- Members and data set names containing USSTAB and LOGAPPL definitions of all terminals that can log on to the system (e.g., SYS1.VTAMLST).
- Members and data set names containing logon mode parameters.

If USSTAB definitions are only used for secure terminals (e.g., terminals that are locally attached to the host or connected to the host via secure leased lines), this is not a finding.

If USSTAB definitions are used for any unsecured terminals (e.g., dial up terminals or terminals attached to the Internet such as TN3270 or KNET 3270 emulation), this is a finding.

Fix Text: Configure USSTAB definitions to be only used for secure terminals.

Only terminals that are locally attached to the host or connected to the host via secure leased lines located in a secured area. Only authorized personnel may enter the area where secure terminals are located.

USSTAB or LOGAPPL definitions are used to control logon from secure terminals. These terminals can log on directly to any VTAM application (e.g., TSO, CICS, etc.) of their choice and bypass Session Manager services. Secure terminals are usually locally attached to the host or connected to the host via a private LAN without access to an external network. Only authorized personnel may enter the area where secure terminals are located.

CCI: CCI-001499

UNCLASSIFIED