UNCLASSIFIED

IBM z/OS ACF2 Security Technical Implementation Guide

Version: 8

Release: 13

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-223419
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223419r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-CE-000010
Rule Title: IBM z/OS Certificate Name Filtering must be implemented with appropriate authorization and documentation.
Legacy ID: V-97535
Legacy ID: SV-106639

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, collect documentation describing each active filter rule and written approval from the ISSM to use the rule.

Issue the following ACF2 commands to list the certificate name filters defined to ACF2:
SET CONTROL(GSO)
SHOW CERTMAP

If no CERTMAP FILTERING TABLES are present, this 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 CERTMAP FILTERING TABLES are present and certificate name filters 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: Define any Certificate Name Filtering rules when required with documentation and approval by the ISSM.

CCI: CCI-000764

Group ID (Vulid): V-223420
Group Title: SRG-OS-000066-GPOS-00034
Rule ID: SV-223420r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-CE-000020
Rule Title: IBM z/OS must not use Expired Digital Certificates.
Legacy ID: SV-106641
Legacy ID: V-97537

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-ACF2 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.

If the digital certificate information indicates that the issuer's distinguished name leads to a DoD PKI Root Certificate Authority or External Certification Authority (ECA), this is not a finding.

Reference the DoD Cyber Exchange website for complete information as to which certificates are acceptable (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: 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-223421
Group Title: SRG-OS-000066-GPOS-00034
Rule ID: SV-223421r868781_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-CE-000030
Rule Title: All IBM z/OS digital certificates in use must have a valid path to a trusted Certification authority.
Legacy ID: SV-106643
Legacy ID: V-97539

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.

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

Check Content:
Execute the CA-ACF2 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 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.

CCI: CCI-000185

CCI: CCI-002470

Group ID (Vulid): V-223422
Group Title: SRG-OS-000001-GPOS-00001
Rule ID: SV-223422r533198_rule
Severity: CAT I

Rule Version (STIG-ID): ACF2-ES-000010
Rule Title: CA-ACF2 OPTS GSO record must be set to ABORT mode.
Legacy ID: SV-106645
Legacy ID: V-97541

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.

Satisfies: SRG-OS-000001-GPOS-00001, SRG-OS-000480-GPOS-00229

Check Content:
From the ISPF Command Shell enter "ACF" to enter ACF2 Command shell.

Enter "SHOW STATE".

If the "GSO OPTS" record show a "MODE= ABORT", this is not a finding.

Fix Text: Configure the GSO Option for "MODE" to equal "ABORT".

CCI: CCI-000015

Group ID (Vulid): V-223423
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223423r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000020
Rule Title: The number of ACF2 users granted the special privilege PPGM must be justified.
Legacy ID: V-97543
Legacy ID: SV-106647

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:
SET LID
SET VERBOSE
LIST IF(PPGM)

If the number of users granted the special privilege PPGM is strictly controlled and limited to systems programmer and operations personnel, this is not a finding.

Fix Text: Ensure that access to the special privilege PPGM is kept to a minimum and limited to systems programmer and operations personnel.

CCI: CCI-000213

Group ID (Vulid): V-223424

Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223424r904401_rule
Severity: CAT III
Rule Version (STIG-ID): ACF2-ES-000030
Rule Title: The number of ACF2 users granted the special privilege OPERATOR must be kept to a strictly controlled minimum.
Legacy ID: V-97545
Legacy ID: SV-106649

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:
ACF
SET LID
SET VERBOSE
LIST IF(OPERATOR)

If the number of users granted the special privilege OPERATOR is strictly controlled and limited to systems programmer and operations personnel, this not a finding.

If the number of users granted the special privilege OPERATOR is not strictly controlled and limited to systems programmer and operations personnel, this is a finding.

Fix Text: Ensure that access to the special privilege "OPERATOR" is kept to a minimum and limited to systems programmer, security manager and operations personnel.

CCI: CCI-000213

Group ID (Vulid): V-223425
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223425r904402_rule
Severity: CAT III
Rule Version (STIG-ID): ACF2-ES-000040
Rule Title: The number of ACF2 users granted the special privilege CONSOLE must be justified.
Legacy ID: V-97547
Legacy ID: SV-106651

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:
ACF
SET LID
SET VERBOSE
LIST IF(ACCTPRIV OR CONSOLE OR OPERATOR OR MOUNT)

If the number of users granted the special privilege CONSOLE is strictly controlled (issued on an as-needed basis), this is not a finding.

If the number of users granted the special privilege CONSOLE is not strictly controlled (issued on an as-needed basis), this is a finding.

Fix Text: Define the CONSOLE attribute with minimum access and it is controlled and documented.

Documentation providing justification for access is maintained and filed with the ISSO and that unjustified access is removed.

CCI: CCI-000213

Group ID (Vulid): V-223426
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223426r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000050
Rule Title: The number of ACF2 users granted the special privilege ALLCMDS must be justified.
Legacy ID: V-97549
Legacy ID: SV-106653

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:
ACF
SET LID
SET VERBOSE
LIST IF(ALLCMDS)

If the number of users granted the special privilege ALLCMDS is strictly controlled and access is granted on an as needed basis, this is not a finding.

If the number of users granted the special privilege ALLCMDS is not strictly controlled and

access is granted on an as needed basis, this is a finding.

Fix Text: Ensure that access to the special privilege ALLCMDS is kept to a minimum and is controlled and documented.

Documentation providing justification for access is maintained and filed with the ISSO.

Remove any unjustified access.

CCI: CCI-000213

Group ID (Vulid): V-223427
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223427r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000060
Rule Title: IBM z/OS system commands must be properly protected.
Legacy ID: V-97551
Legacy ID: SV-106655

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 input line enter:
SET RESOURCE(OPR)
SET VERBOSE
LIST LIKE(MVS-)

NOTE: If CLASMAP defines OPERCMDS as anything other than the default of TYPE(OPR), replace OPR with the appropriate three letters.

If the MVS resource is defined to the OPERCMDS class with a default access of PREVENT, and all access logged, i.e., MVS.** is defined with access of PREVENT, this is not finding.

If Access to z/OS system commands 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) as determined in the Documented site Security Plan, this is not a finding.

Note: Display commands and others as deemed by the site IAW site security plan may be allowed for all users with no logging. The (MVS.SEND) Command will not be a finding if used by all.

Fix Text: Configure z/OS Sensitive System Commands to be defined to the OPERCMDS resource class. Only limited number of authorized people are able to issue these commands. All access is logged.

Configure the MVS resource to be defined to the OPERCMDS class with a default access of PREVENT, all access is logged, and access is restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users).

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

Example for ACF2:
$KEY(MVS) TYPE(OPR)
ACTIVATE.- UID(sysprgmr) LOG
ACTIVATE.- UID(*) PREVENT

SET R(OPR)
COMPILE 'ACF2.MVA.OPR(MVS)' STORE

F ACF2,REBUILD(OPR)

CCI: CCI-000213

Group ID (Vulid): V-223428
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223428r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000070

Rule Title: IBM z/OS Sensitive Utility Controls must be properly defined and protected.
Legacy ID: SV-106657
Legacy ID: V-97553

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 detailed in the table.

If the ACF2 resources are defined with a default access of PREVENT, this is not a finding.

If the ACF2 resource access authorizations restrict access to the appropriate personnel according to the site security plan, this not a finding.

If the ACF2 resource logging is correctly specified, 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.

Fix Text: Refer to the Site Security plan for Sensitive Programs/Utilities for lists the resources, access requirements, and logging requirements for Sensitive Utilities.

Configure ACF2 resources to be defined with a default access of PREVENT.

Configure ACF2 resource access authorizations to restrict access to the appropriate personnel.

Configure ACF2 resource logging to be correctly specified.

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

$KEY(AHLGTF) TYPE(PGM)
UID(stcg) LOG
UID(*) PREVENT

F ACF2,REBUILD(PGM)

CCI: CCI-000213

Group ID (Vulid): V-223429
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223429r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000080
Rule Title: CA-ACF2 NJE GSO record value must indicate validation options that apply to jobs submitted through a network job entry subsystem (JES2, JES3, RSCS).
Legacy ID: SV-106659
Legacy ID: V-97555

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 ACF input screen enter:
SET CONTROL(GSO)
LIST LIKE(NJE-)

If the GSO NJE record values conform to the following requirements, this is not a finding.

Specifies ACF2 validation options that apply to jobs submitted through a network job entry subsystem (JES2, JES3, RSCS).

DFTLID() INHERIT NODEMASK(-) ENCRYPT VALIN(YES) NOVALOUT

NOTE: For NJE nodes that are incompatible with the XDES algorithm, discrete NJE records will

be created with NOENCRYPT.
NOTE: Local changes will be documented in writing with supporting documentation.

Fix Text: Configure ACF2 validation options that apply to jobs submitted through a network job entry subsystem (JES2, JES3, RSCS) as follows:

DFTLID()
INHERIT
NODEMASK(-)
ENCRYPT
VALIN(YES)
NOVALOUT

NOTE: For NJE nodes that are incompatible with the XDES algorithm, discrete NJE records will be created with NOENCRYPT.

NOTE: Local changes will be justified in writing with supporting documentation.

CCI: CCI-000213

Group ID (Vulid): V-223430
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223430r868783_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000090
Rule Title: CA-ACF2 must protect Memory and privileged program dumps in accordance with proper security requirements.
Legacy ID: SV-106661
Legacy ID: V-97557

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 input screen enter:

SET RESOURCE (FAC)
SET VERBOSE
LIST LIKE (IEAABD-)
NOTE: If CLASMAP defines FACILITY as anything other than the default of TYPE(FAC), replace FAC with the appropriate three letters.

If the IEAABD. resource and/or generic equivalent is defined with PREVENT access and that access is not available to any user, this is not a finding.

If the IEAABD.DMPAUTH. resource and/or generic equivalent is defined and access with SERVICE(READ) is limited to authorized users that have a valid job duties requirement for access, this is not a finding.

If the IEAABD.DMPAUTH. resource and/or generic equivalent is defined and access with the SERVICE(UPDATE) or greater is restricted to only systems personnel and that 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 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.)

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 ACF2 resources are defined with a default access of PREVENT.

Ensure that no access is given to IEAABD. resource.

Example:
$KEY(IEAABD) TYPE(FAC)
- UID(*) PREVENT

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:
$KEY(IEAABD) TYPE(FAC)
DMPAUTH.- UID(sysprgmr) SERVICE(UPDATE) LOG
DMPAUTH.- UID(authusers) SERVICE(READ)
DMPAUTH.- UID(*) PREVENT

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

Example:
$KEY(IEAABD) TYPE(FAC)
DMPAKEY.- UID(sysprgmr) LOG
DMPAKEY.- UID(*) PREVENT

CCI: CCI-000213

Group ID (Vulid): V-223431
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223431r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000100
Rule Title: CA-ACF2 must properly define users that have access to the CONSOLE resource in the TSOAUTH resource class.
Legacy ID: SV-106663
Legacy ID: V-97559

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:
NOTE: If CLASMAP defines TSOAUTH or OPERCMDS as anything other than the default of TYPE(TSO) or TYPE(OPR), replace TSO or OPR below with the appropriate three letters.

If the CONSOLE resource is not defined to the TSOAUTH resource class, this is not a finding.

At the discretion of the ISSO, users may be allowed to issue z/OS system commands from a TSO session. With this in mind, configure the following for users granted the CONSOLE resource in the TSOAUTH resource class or users assigned the CONSOLE attribute:

Logonids are restricted to the INFO level on the AUTH field specified in the OPERPARM segment of the user profile record.
Logonids are restricted to READ access to the MVS.MCSOPER.userid resource defined in the OPERCMDS resource class (i.e., resource rules for TYPE(OPR)).

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

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

Fix Text: Configuration should ensure that all users that have access to the CONSOLE resource in the TSOAUTH resource class are properly defined.

Ensure the CONSOLE resource is not defined to the TSOAUTH resource class.

Example:
$KEY(CONSOLE) TYPE(TSO)
- UID(*) PREVENT

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 CONSOLE resource in the TSOAUTH resource class or users assigned the CONSOLE attribute:

Logonids are restricted to the INFO level on the AUTH field specified in the OPERPARM segment of the user profile record.

Logonids are restricted to READ access to the MVS.MCSOPER.userid resource defined in the

OPERCMDS resource class (i.e., resource rules for TYPE(OPR)).

Example:
$KEY(MVS) TYPE(OPR)
MCSOPER.logonid UID(sysprgmr) SERVICE(READ) ALLOW

COMPILE ' ACF2.MVA.OPR(MVS)' STORE

F ACF2,REBUILD(OPR)

CCI: CCI-000213

Group ID (Vulid): V-223433
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223433r918576_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000120
Rule Title: CA-ACF2 must limit access to SYSTEM DUMP data sets to appropriate authorized users.
Legacy ID: V-97563
Legacy ID: SV-106667

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:
Ask the system administrator and/or DASD administrator to determine the System Dump data sets.

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

If ACF2 data set rules for System Dump data sets do not restrict READ, WRITE, and/or ALLOCATE access to only systems programming personnel, this is a finding.

If ACF2 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

Group ID (Vulid): V-223434
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223434r853499_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000130
Rule Title: CA-ACF2 must limit access to SYS(x).TRACE to system programmers only.
Legacy ID: V-97565
Legacy ID: SV-106669

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:
Execute a data set 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-223435
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223435r918579_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000140
Rule Title: CA-ACF2 allocate access to system user catalogs must be properly protected.
Legacy ID: V-97567
Legacy ID: SV-106671

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:
From the ISPF Command Shell, enter:
LISTCat USERCATALOG NAME NOPREFIX

Review the ACF2 data set rules for each usercatalog defined.

If the data set rules for User Catalogs do not restrict ALLOCATE 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:
- 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 above is true, this is not a finding.

If the data set rules for User Catalogs do not specify that all (i.e., failures and successes)

ALLOCATE access will be logged, this is 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 datasets, WRITE 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 ACF2 rules for allocate access to USER CATALOGS, limited to system programmers only, and all allocate access is logged.

Configure ACF2 rules for the USER CATALOGS to allow any Products or procedures system programmer access for system-level maintenance that meets 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 datasets WRITE access is required for user operation.

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223436
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223436r836693_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000150
Rule Title: ACF2 Classes required to properly security the z/OS UNIX environment must be ACTIVE.
Legacy ID: V-97569
Legacy ID: SV-106673

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:
ACF
SET CONTROL(GSO)
SHOW CLASMAP

If the CLASMAP DEFINITIONS list does not include entries for the FACILITY, SURROGAT, and UNIXPRIV resource classes, this is a finding.

NOTE: TYPE CODES values should be unique for each resource. The default TYPE CODE values should be FAC, SUR, and UNI.

Fix Text: Define the CLASMAP DEFINITIONS to include entries for the FACILITY, SURROGAT, and UNIXPRIV resource classes.

NOTE: TYPE CODES values should be unique for each resource. The default TYPE CODE values should be FAC, SUR, and UNI.

Example:
TSO ACF
SHOW CLASMAP

ACF
SET CONTROL(GSO)
INSERT CLASMAP.FACILITY RESOURCE(FACILITY) RSRCTYPE(FAC) ENTITYTLN (39)

CCI: CCI-000213

Group ID (Vulid): V-223437
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223437r533198_rule
Severity: CAT II

Rule Version (STIG-ID): ACF2-ES-000160
Rule Title: Access to IBM z/OS special privilege TAPE-LBL or TAPE-BLP must be limited and/or justified.
Legacy ID: V-97571
Legacy ID: SV-106675

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:
ACF
SET LID
SET VERBOSE
LIST IF(TAPE-LBL OR TAPE-BLP)

If the number of users granted the special privileges TAPE-LBL or TAPE-BLP is strictly controlled and limited to systems programmer and operations personnel, this is not a finding.

If the number of users granted the special privileges TAPE-LBL or TAPE-BLP is not strictly controlled and limited to systems programmer and operations personnel, this is a finding.

Fix Text: The ISSO will ensure Logonids with the TAPE-LBL or TAPE-BLP are kept to a minimum and are controlled and documented.

Review all LOGONIDs with these attributes.

Tape label bypass (BLP) privileges will be restricted at the user level. Specify one of the following two logonid privileges to grant a user access to BLP processing:

User LID Record:

TAPE-LBL
TAPE-BLP

It is possible to grant selected programs to bypass tape label processing regardless of the BLP related privilege of the logonid executing the program. This capability will not be used due to the requirement that accounting of BLP processing be done at the user level. Do not utilize the GSO BLPPGM record.

CCI: CCI-000213

Group ID (Vulid): V-223438
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223438r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000170
Rule Title: CA-ACF2 must limit access to System page data sets (i.e., PLPA, COMMON, and LOCALx) to system programmers.
Legacy ID: SV-106677
Legacy ID: V-97573

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 data set list of access for System page data sets (i.e., PLPA, COMMON, and LOCALx).

If the ESM data set rules for System page data sets (i.e., PLPA, COMMON, and LOCALx) do not restrict access to only systems programming personnel, this is 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

Group ID (Vulid): V-223439
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223439r861164_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000180
Rule Title: IBM z/OS must protect dynamic lists in accordance with proper security requirements.
Legacy ID: SV-106679
Legacy ID: V-97575

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 a command input screen enter:

SET RESOURCE (FAC)
SET VERBOSE
LIST LIKE (CSV-)

NOTE: If CLASMAP defines FACILITY as anything other than the default of TYPE(FAC), replace FAC with the appropriate three letters.

If the ACF2 resources and/or generic equivalent are defined with a default access of PREVENT, this is not a finding.

If the ACF2 resources and/or generic equivalent identified below will be defined with LOG and SERVICE(UPDATE) access restricted to system programming personnel, this is not a finding.

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

If the ACF2 CSVDYNEX.LIST resource and/or generic equivalent will be defined with LOG and SERVICE(UPDATE) access restricted to system programming personnel, this is not a finding.

If the ACF2 CSVDYNEX.LIST resource and/or generic equivalent will be defined with SERVICE(READ) access restricted to auditors, this is not a finding.

If the products CICS and/or CONTROL-O are on the system, the ACF2 access to the CSVLLA resource and/or generic equivalent will be defined with LOG and SERVICE(UPDATE) access restricted to the CICS and CONTROL-O STC logonids, this is not a finding.

If any software product requires access to dynamic LPA updates on the system, the ACF2 access to the CSVDYLPA resource and/or generic equivalent will be defined with LOG and SERVICE(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, this is not a finding.

Note: In the above, SERVICE(UPDATE) can be substituted with ADD, CONTROL, or LOG/ALLOW. Review the rules definitions in the ACF2 documentation when specifying SERVICE(UPDATE).

Fix Text: Configure the Dynamic List resources to be 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.

Note: The resource class, resources, and/or resource prefixes identified below are examples of a possible installation. The resource class, actual resources, 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 required CSV-prefixed Facility Class resources are listed below. These resources and/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.DELETE.-
CSVDYNEX.-
CSVDYNEX.LIST
CSVDYNL.-
CSVDYNL.UPDATE.LNKLST
CSVLLA.-

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

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

$KEY(CSVAPF) TYPE(FAC)
MVS.SETPROG.- UID(sysprgmr) LOG
MVS.SETPROG.FORMAT.DYNAMIC.- UID(sysprgmr) LOG
MVS.SETPROG.FORMAT.STATIC.- UID(sysprgmr) LOG
MVS.SETPROG.FORMAT.- UID(sysprgmr) LOG
MVS.SETPROG.FORMAT.- UID(*) PREVENT
- UID(sysprgmr) LOG
- UID(*) PREVENT

SET R(FAC)
COMPILE 'ACF2.xxxx.FAC(CSVAPF)' STORE

F ACF2,REBUILD(FAC)

The CSVDYLPA.ADD resource can be permitted to BMC Mainview, CA 1, and CA Common Services STC logonids with LOG and SERVICE(UPDATE) access.

The CSVDYLPA.DELETE resource can be permitted to CA 1 and CA Common Services STC

logonids with LOG and SERVICE(UPDATE) access.

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

```
$KEY(CSVDYLPA) TYPE(FAC)
ADD.- UID(sysprgmr) LOG SERVICE(UPDATE)
ADD.- UID(BMC Mainview STC) LOG SERVICE(UPDATE)
ADD.- UID(CA 1 STC) LOG SERVICE(UPDATE)
ADD.- UID(CCS STC) LOG SERVICE(UPDATE)
DELETE.- UID(sysprgmr) LOG SERVICE(UPDATE)
DELETE.- UID(CA 1 STC) LOG SERVICE(UPDATE)
DELETE.- UID(CCS STC) LOG SERVICE(UPDATE)
- UID(sysprgmr) LOG
- UID(*) PREVENT

SET R(FAC)
COMPILE 'ACF2.xxxx.FAC(CSVDYLPA)' STORE

F ACF2,REBUILD(FAC)
```

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

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

Sample commands are shown here to accomplish this:

```
$KEY(CSVDYNEX) TYPE(FAC)
LIST.- UID(sysprgmr) LOG
LIST.- UID(auditor) SERVICE(READ) ALLOW
- UID(sysprgmr) LOG
- UID(*) PREVENT

SET R(FAC)
COMPILE 'ACF2.xxxx.FAC(CSVDYNEX)' STORE

F ACF2,REBUILD(FAC)
```

The CSVLLA resource can be permitted to CICS and CONTROL-O STC logonids with LOG and SERVICE(UPDATE) access.

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

```
$KEY(CSVLLA) TYPE(FAC)
- UID(sysprgmr) LOG
```

- UID(CICS STC logonids) LOG SERVICE(UPDATE)
- UID(CONTROL-O STC logonid) LOG SERVICE(UPDATE)
- UID(*) PREVENT

SET R(FAC)
COMPILE 'ACF2.xxxx.FAC(CSVLLA)' STORE

F ACF2,REBUILD(FAC)

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223440
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223440r853504_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000190
Rule Title: IBM z/OS Libraries included in the system REXXLIB concatenation must be properly protected.
Legacy ID: SV-106681
Legacy ID: V-97577

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 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 UPDATE and/or ALTER access (i.e., successes and failures).

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223441
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223441r918582_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000200
Rule Title: CA-ACF2 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: SV-106683
Legacy ID: V-97579

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:
The ACF2 data set rules for SYS1.UADS restrict ALLOCATE access to only z/OS systems programming personnel.

The ACF2 data set rules for SYS1.UADS restrict READ and/or WRITE access to z/OS systems programming personnel and/or security personnel.

The ACF2 data set rules for SYS1.UADS restrict READ access to auditors as documented in the Security Plan.

The ACF2 data set rules for SYS1.UADS specify that all (i.e., failures and successes) data set access authorities (i.e., READ, WRITE, ALLOCATE, and CONTROL) will be logged.

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/or WRITE 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 dataset access is logged.

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223442
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223442r861165_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000210
Rule Title: CA-ACF2 must limit all system PROCLIB data sets to appropriate authorized users.
Legacy ID: SV-106685
Legacy ID: V-97581

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 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 ensure that 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 are restricted 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 is what 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-223443
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223443r836648_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000220
Rule Title: CA-ACF2 access to the System Master Catalog must be properly protected.
Legacy ID: V-97583
Legacy ID: SV-106687

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:
- 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 above is true, this is not a finding.

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 master catalog to only allow access above "READ" to systems programmers and those authorized by the Site Security Plan.

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

Configure ESM rules for the system 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

Group ID (Vulid): V-223444
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223444r853509_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000230
Rule Title: IBM z/OS MCS consoles access authorization(s) for CONSOLE resource(s) must be properly protected.
Legacy ID: V-97585
Legacy ID: SV-106689

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 the proper CONSOLxx member of SYS1.PARMLIB.

From a ACF Command screen enter:
ACF
SET RESOURCE(CON)
SET VERBOSE
LIST LIKE(-)

NOTE: If CLASMAP defines CONSOLE as anything other than the default of TYPE(CON),

replace CON below with the appropriate three letters.

If each console in the CONSOLxx member is defined to ACF2 with a corresponding resource rule for TYPE(CON), this is not a finding.

If each TYPE(CON) rule is defined with PREVENT access by default, this is not a finding.

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

If access authorization for CONSOLE resources restricts READ access to operations and system programming personnel or authorized personnel, this is not a finding.

Fix Text: Configuration should ensure that all MCS consoles are defined to the CONSOLE resource class and READ access is limited to operators and system programmers.

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 ACF2 with a corresponding resource rule for TYPE(CON).

Each TYPE(CON) rule is defined with PREVENT access by default.

The logonid associated with each console has READ access to the corresponding resource defined in the CONSOLE resource class.

Access authorization for CONSOLE resources restricts READ access to operations and system programming personnel or authorized personnel.

Example:
$KEY(MZNC20) TYPE(CON)
USERDATA(CONSOLE ID SECURITY)
UID(sysprgmr) ALLOW
UID(oper) ALLOW
UID(MZNC20) ALLOW DATA(MZNC20 CONSOLE LOGONID ACCESS REQUIREMENTS)
UID(*) PREVENT

SET R(CON)
COMPILE 'ACF2.MZN.CON(MZNC20)' STORE

F ACF2,REBUILD(CON)

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223445
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223445r918584_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000240
Rule Title: CA-ACF2 must limit Write or greater access to SYS1.NUCLEUS to system programmers only.
Legacy ID: V-97587
Legacy ID: SV-106691

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:
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 SYS1.NUCLEUS do not restrict WRITE and/or ALLOCATE 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 and/or ALLOCATE 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 update and allocate access to SYS1.NUCLEUS to be limited to system programmers only and all update and allocate access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223446
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223446r918586_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000250
Rule Title: CA-ACF2 must limit Write or greater access to SYS1.LPALIB to system programmers only.
Legacy ID: V-97589
Legacy ID: SV-106693

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

- The ACF2 data set rules for SYS1.LPALIB do not restrict WRITE and/or ALLOCATE access to only z/OS systems programming personnel.
- The ACF2 data set rules for SYS1.LPALIB do not specify that all (i.e., failures and successes) WRITE and/or ALLOCATE 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 update and allocate access to SYS1.LPALIB to be limited to system programmers only and all update and allocate access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223447
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223447r918589_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000260
Rule Title: CA-ACF2 must limit Write or greater access to SYS1.IMAGELIB to system programmers.
Legacy ID: V-97591
Legacy ID: SV-106695

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.

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 must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

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 allow inappropriate access.

The ACP data set rules for SYS1.IMAGELIB do not restrict WRITE and/or ALLOCATE 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 and/or ALLOCATE access will be logged.

Fix Text: Configure WRITE and/or ALLOCATE access to SYS1.IMAGELIB to be limited to system programmers only and all update and allocate 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-223448
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223448r861166_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000270
Rule Title: CA-ACF2 must limit Write or greater access to Libraries containing EXIT modules to system programmers only.
Legacy ID: V-97593
Legacy ID: SV-106697

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.

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 must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

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:
Examine the system for active exit modules. You may need system administrator help for this. Third-party software products 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 UPDATE and ALLOCATE 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 UPDATE and ALLOCATE 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. See 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 update and alter 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-223449
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223449r918591_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000280
Rule Title: CA-ACF2 must limit Write and Allocate access to all APF-authorized libraries to system programmers only.
Legacy ID: SV-106699
Legacy ID: V-97595

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.

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 must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

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 is true, this is a finding.

- The ACP data set rules for APF libraries do not restrict WRITE and/or ALLOCATE 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 and/or ALLOCATE 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 Update and Allocate access to all APF-authorized libraries to be limited to system programmers only and all update and alter access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223450
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223450r918593_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000290
Rule Title: CA-ACF2 must limit Write or greater access to all LPA libraries to system programmers only.
Legacy ID: SV-106701
Legacy ID: V-97597

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 and/or ALLOCATE 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 and/or ALLOCATE 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 update and allocate access to all LPA libraries to be limited to system programmers only and all update and allocate access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223451
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223451r918595_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000300
Rule Title: CA-ACF2 must limit Write and Allocate access to LINKLIST libraries to system programmers only.
Legacy ID: SV-106703
Legacy ID: V-97599

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 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 and/or ALLOCATE 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 and/or ALLOCATE 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 update and allocate access to LINKLIST libraries to be limited to system programmers only and all update and allocate access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223452
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223452r918597_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000310
Rule Title: CA-ACF2 must limit Write and allocate access to all system-level product installation libraries to system programmers only.
Legacy ID: SV-106705
Legacy ID: V-97601

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 used 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 ACF2 data set rules for system-level product installation libraries (e.g., SMP/E CSIs) do not restrict WRITE and/or ALLOCATE 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-223453
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223453r918599_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000320
Rule Title: CA-ACF2 must limit Write or greater access to SYS1.SVCLIB to system programmers only.
Legacy ID: V-97603
Legacy ID: SV-106707

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.

ACF2 data set rules for SYS1.SVCLIB restrict WRITE and/or ALLOCATE access to only z/OS systems programming personnel.

ACF2 data set rules for SYS1.SVCLIB specify that all (i.e., failures and successes) WRITE and/or ALLOCATE access will be logged.

Fix Text: Configure update and allocate access to SYS1.SVCLIB to be limited to system programmers only and all Update and Allocate 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-223454
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223454r918602_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000330
Rule Title: CA-ACF2 Access to SYS1.LINKLIB must be properly protected.
Legacy ID: V-97605
Legacy ID: SV-106709

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 must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

The operating system or software configuration management utility must enforce control of software installation by users based upon what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect) by the organization.

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

GPOS-00125, SRG-OS-000362-GPOS-00149

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

If the ACF2 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, and ALLOCATE access to only systems programming personnel, this is a finding.

If data set rules for SYS1.LINKLIB do not restrict READ and WRITE 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 and/or ALLOCATE access will be logged, this is a finding.

Fix Text: Configure the ACF2 rules for SYS1.LINKLIB limit access to system programmers only and all update and allocate access is logged.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-001812

CCI: CCI-002235

Group ID (Vulid): V-223455
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223455r861167_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000340
Rule Title: CA-ACF2 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: V-97607
Legacy ID: SV-106711

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

If the ESM dataset rules for the SMF dump/backup files do not 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 the 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: Define WRITE or greater access to data sets used to back up and/or dump SMF collection files to be limited to system programmers and/or batch jobs that perform SMF dump processing. Ensure that all data set access is logged.

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

Define READ Access to data sets used to back up and/or dumpSMF collection files to be limited

to auditors and others approved by the ISSM.

Ensure that all WRITE or greater access authority to SMF history files will be logged using the ESM's facilities.

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 back up and/or dump SMF Collection Files.

In z/OS systems, SMF data is the ultimate record of system activity. Therefore, SMF data is of the most sensitive and critical nature. While the length of time for which SMF data will be retained is not specifically regulated, it is imperative that the information is available for the longest possible time period in case of subsequent investigations. The statute of limitations varies according to the nature of a crime. It may vary by jurisdiction, and some crimes are not subject to a statute of limitations. Apply the following guidelines to the retention of SMF data for all DOD systems:

(a) Retain at least two (2) copies of the SMF data.
(b) Maintain SMF data for a minimum of one year.
(c) All WRITE or greater access authority to SMF history files will be logged using the ACP's facilities. Only systems programming personnel and batch jobs that perform SMF functions will be authorized to update the SMF files.

CCI: CCI-000213

CCI: CCI-001314

CCI: CCI-002235

Group ID (Vulid): V-223456
Group Title: SRG-OS-000324-GPOS-00125
Rule ID: SV-223456r877392_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000350
Rule Title: CA-ACF2 LOGONIDs must not be defined to SYS1.UADS for non-emergency use.
Legacy ID: V-97609
Legacy ID: SV-106713

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 SYS1.UADS userids are limited and reserved for emergency purposes only, this is not 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-223457
Group Title: SRG-OS-000324-GPOS-00125
Rule ID: SV-223457r929597_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000370
Rule Title: IBM z/OS IEASYMUP resource must be protected in accordance with proper security requirements.
Legacy ID: V-97611
Legacy ID: SV-106715

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 ACF Command screen enter:
SET RESOURCE(FAC)
LIST IEASYMUP

If the accesses for IEASYMUP resources and/or generic equivalent are properly restricted, this is not a finding.

The ACF2 resources are defined with a default access of PREVENT.
The ACF2 resource access authorizations specify SERVICE(UPDATE) and/or greater access to only DASD administrators, Tape Library personnel, and system programming personnel.
The ACF2 resource access authorizations specify logging.

Fix Text: Configure the System level symbolic resources to be 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 the above personnel with LOG and SERVICE(UPDATE) and/or greater access.

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

$KEY(IEASYMUP) TYPE(FAC)
- UID(<dasd>) SERVICE(UPDATE) LOG
- UID(<sysprgmr>) SERVICE(UPDATE) LOG
- UID(<tape librarian>) SERVICE(UPDATE) LOG
- UID(*) PREVENT

SET R(FAC)
COMPILE 'ACF2.FAC(IEASYMUP)' STORE

F ACF2,REBUILD(FAC)

CCI: CCI-002235

Group ID (Vulid): V-223458
Group Title: SRG-OS-000324-GPOS-00125
Rule ID: SV-223458r877392_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000380
Rule Title: CA-ACF2 must limit Update and Allocate access to system backup files to system programmers and/or batch jobs that perform DASD backups.
Legacy ID: V-97613
Legacy ID: SV-106717

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:
Collect from the storage management group the identification of the DASD backup files and all associated storage management userids/LIDs/ACIDs.

If ESM data set rules for system DASD backup files do not restrict UPDATE and ALLOCATE 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-002235

Group ID (Vulid): V-223459
Group Title: SRG-OS-000324-GPOS-00125
Rule ID: SV-223459r877392_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000390
Rule Title: ACF2 PPGM GSO record value must specify protected programs that are only executed by privileged users.
Legacy ID: SV-106719
Legacy ID: V-97615

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 ACF command screen enter:
SET CONTROL(GSO)
LIST LIKE(PPGM-)

Refer to the table of Sensitive Utilities resources and/or generic equivalent as detailed in the table.

If all applicable programs or their generic equivalent referenced below are represented by GSO PPGM record values, 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.

Fix Text: Configure the PPGM GSO value indicating protected programs that are only executed by privileged users in the table below.

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.

Define protected programs that can only be executed by privileged users.

PGM MASK(pgm mask1, ...,pgm-mask255)

Example:
SET C(GSO)
INSERT PPGM PGM-MASK(<program name or generic equivalent>)

F ACF2,REFRESH(PPGM)

CCI: CCI-002235

Group ID (Vulid): V-223462
Group Title: SRG-OS-000329-GPOS-00128
Rule ID: SV-223462r853526_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000430
Rule Title: The CA-ACF2 PSWD GSO record values for MAXTRY and PASSLMT must be properly set.
Legacy ID: SV-106725
Legacy ID: V-97621

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 an ACF command screen enter:
SET CONTROL(GSO)
SHOW PSwdopts

If "MAXTRY" is set to "3", this is not a finding.

If "PASSLMT" is set to "3", this is not a finding.

Fix Text: Configure the GSO option "MAXTRY" to equal "3".
Configure the GSO option "PASSLMT" to equal "3".

CCI: CCI-002238

Group ID (Vulid): V-223463
Group Title: SRG-OS-000063-GPOS-00032
Rule ID: SV-223463r918604_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000440
Rule Title: IBM z/OS SYS1.PARMLIB must be properly protected.
Legacy ID: SV-106727
Legacy ID: V-97623

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.

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-000324-GPOS-00125, SRG-OS-000337-GPOS-00129, SRG-OS-

000362-GPOS-00149

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

If the ACF2 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, and ALLOCATE access to only systems programming personnel, this is a finding.

If data set rules for SYS1.PARMLIB do not restrict READ and WRITE 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 and/or ALLOCATE access will be logged, this is a finding.

Fix Text: Configure access rules for SYS1.PARMLIB as follows:
Systems programming personnel will be authorized to update and alter the SYS1.PARMLIB concatenation.
Domain level security administrators can be authorized to update the SYS1.PARMLIB concatenation.
System Level Started Tasks, authorized Data Center personnel, and auditor can be authorized read access by the ISSO.
All update and alter access is logged.

CCI: CCI-000171

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-001812

CCI: CCI-001914

CCI: CCI-002235

Group ID (Vulid): V-223464
Group Title: SRG-OS-000364-GPOS-00151
Rule ID: SV-223464r853528_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000450
Rule Title: CA-ACF2 must be installed, functional, and properly configured.
Legacy ID: V-97625
Legacy ID: SV-106729

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. You can use IBM SDSF or the system Log.

If CA-ACF2 is active, this is not a finding.

Fix Text: Assure that CA-ACF2 is active on the system.

CCI: CCI-001813

Group ID (Vulid): V-223465
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223465r918606_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000470

Rule Title: CA-ACF2 must limit Write and allocate access to the JES2 System data sets (e.g., Spool, Checkpoint, and Initialization parameters) to system programmers only.
Legacy ID: V-97629
Legacy ID: SV-106733

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, SRG-OS-000259-GPOS-00100

Check Content:
The ACF2 data set rules for the JES2 System data sets (e.g., Spool, Checkpoint, and Initialization parameters) do not restrict WRITE and/or ALLOCATE access to only z/OS systems programming personnel.

The ACF2 data set rules for the JES2 System data sets (e.g., Spool, Checkpoint, and Initialization parameters) allow inappropriate access not documented and approved by the ISSO.

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

If either of the above are true, 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.

Access other than this should be documented and approved by the ISSO.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223466
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223466r853530_rule
Severity: CAT III
Rule Version (STIG-ID): ACF2-ES-000480
Rule Title: CA-ACF2 must limit Write or greater access to libraries that contain PPT modules to system programmers only.
Legacy ID: V-97631
Legacy ID: SV-106735

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 must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

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 ESM data set rules for libraries that contain PPT modules do not restrict UPDATE and ALLOCATE access to only z/OS systems programming personnel.
-The ESM data set rules for libraries that contain PPT modules do not specify that all UPDATE

and ALLOCATE access will be logged.

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

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223467
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223467r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000490
Rule Title: The EXITS GSO record value must specify the module names of site written ACF2 exit routines.
Legacy ID: V-97633
Legacy ID: SV-106737

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 ACF Command enter:
SET CONTROL(GSO)
LIST LIKE(EXIT-)

If the GSO EXITS record values conform to the following requirements, this is not a finding.

Specifies the module names of site written ACF2 exit routines.

NOTE: The DSNPOST exit is optional and is not required to be specified in the GSO EXITS record. DSNPOST(module) SEVPRE(SEVPRE01) SEVPOST(SEVPST01)
NOTE: No other exits are authorized at this time.
NOTE: Local changes will be documented in writing with supporting documentation.

If there is any deviation from the above requirements in the GSO EXITS record values, this is a finding.

Fix Text: Configure the EXITS GSO value to specify the module names of site written ACF2 exit routines.

Specifies the module names of site written ACF2 exit routines.

NOTE: The DSNPOST exit is optional and is not required to be specified in the GSO EXITS record.

DSNPOST(module) SEVPRE(SEVPRE01) SEVPOST(SEVPST01)

Example:
SET C(GSO)
INSERT EXITS DSNPOST(module) SEVPRE(SEVPRE01) SEVPOST(SEVPST01)

F ACF2,REFRESH(EXITS)

NOTE: No other exits are authorized at this time.

NOTE: Local changes will be justified in writing with supporting documentation.

CCI: CCI-000366

Group ID (Vulid): V-223468
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223468r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000500
Rule Title: The CA-ACF2 LOGONID with the REFRESH attribute must have procedures for utilization.
Legacy ID: V-97635
Legacy ID: SV-106739

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 ACF Command screen enter:

SET LID
LIST IF(REFRESH)

If procedures exist to utilize the logonid with the REFRESH attribute to refresh ACF2 global options, this is not a finding.

Example:
When the ISSO determines it necessary to refresh the ACF2 global options, the ISSO will do the following:

-Activate the REFRESH ID with the following setting(s):
NOSUSPEND
NOPSWD EXP
PASSWORD(new password)

-Instruct Operations to perform the REFRESH.

-Deactivate the REFRESH ID with the following setting:
SUSPEND

If no procedures exist in accordance with the STIG requirements to utilize the logonid with the REFRESH attribute to refresh ACF2 global options, this is a finding.

Fix Text: Review security procedures for defining LOGONIDs and develop documentation of requirements for the LOGONID associated with the REFRESH attribute.

Example:
When the ISSO determines it necessary to refresh the ACF2 global options, the ISSO will do the following:

-Activate the REFRESH ID with the following setting(s):
NOSUSPEND
NOPSWD EXP
PASSWORD(new password)

-Instruct Operations to perform the REFRESH.

-Deactivate the REFRESH ID with the following setting:
SUSPEND

CCI: CCI-000225

CCI: CCI-000366

Group ID (Vulid): V-223469
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223469r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000510
Rule Title: IBM z/OS TSO GSO record values must be set to the values specified.
Legacy ID: V-97637
Legacy ID: SV-106741

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 ACF Command screen enter:
SET CONTROL(GSO)
LIST TSO

If the GSO TSO record values conform to the following requirements, this is not a finding.

ACCOUNT(1)
BYPASS(#)
CHAR(BS)
CMDLIST()
NOIKJEFLD1
LINE(ATTN)
LOGONCK
PERFORM(0)
PROC(site defined)
NOQLOGON
REGION(site defined)
SUBCLSS()
SUBHOLD()
SUBMSG()
TIME(0)
TSOSOUT(A)
UNIT(SYSDA)
WAITIME(1-60)

Fix Text: Configure the GSO TSO record values to conform to the following requirements.

ACCOUNT(1)
BYPASS(#)
CHAR(BS)
CMDLIST()
NOIKJEFLD1
LINE(ATTN)
LOGONCK
PERFORM(0)
PROC(site defined)
NOQLOGON
REGION(site defined)
SUBCLSS()
SUBHOLD()
SUBMSGC()
TIME(0)
TSOSOUT(A)
UNIT(SYSDA)
WAITIME(1-60)

Example:
SET C(GSO)
INSERT TSO ACCOUNT(1) BYPASS(#) CHAR(BS) CMDLIST() NOIKJEFLD1
LINE(ATTN) LOGONCK PERFORM(0) PROC(IKJACCNT) NOQLOGON REGION(4,096)
SUBCLSS() SUBHOLD() SUBMSGC() TIME(0) TSOGNAME() TSOSOUT(A)
UNIT(SYSDA) WAITIME(60)

F ACF2,REFRESH(TSO)

CCI: CCI-000366

CCI: CCI-001133

Group ID (Vulid): V-223470
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223470r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000520
Rule Title: IBM z/OS procedures must restrict ACF2 LOGONIDs with the READALL attribute to auditors and/or authorized users.
Legacy ID: V-97639
Legacy ID: SV-106743

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 ACF Command line enter:
SET LID
LIST IF(READALL)

If procedures are in place to ensure logonids with the READALL attribute are used and controlled in accordance with the DISA requirements, this is not a finding.

The READALL privilege is available for actual auditing of system data. It gives the capability of looking at every data set on the system despite the data set rules. Its use is strongly discouraged. Always grant access through the use of standard data set access rules. Under no circumstances will the privilege be used as a convenience to the person maintaining the rule sets. Only use this privilege when absolutely necessary, and only give it to auditors. Remove the privilege once the audit is complete. Fully document the granting and revoking of the access.

Fix Text: Develop procedures to control Logonids with the READALL attribute.

The READALL privilege is available for actual auditing of system data. It gives the capability of looking at every data set on the system despite the data set rules. Its use is strongly discouraged. Always grant access through the use of standard data set access rules. Under no circumstances will the privilege be used as a convenience to the person maintaining the rule sets. Only use this privilege when absolutely necessary, and only give it to auditors. Remove the privilege once the audit is complete. Fully document the granting and revoking of the access.

CCI: CCI-000366

Group ID (Vulid): V-223471
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223471r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000530
Rule Title: IBM z/OS must have the RULEVLD and RSRCVLD attributes specified for LOGONIDs with the SECURITY attribute.
Legacy ID: V-97641
Legacy ID: SV-106745

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 ACF Command screen enter:
SET LID
LIST IF(SECURITY)

If all logonids with the SECURITY attribute also have the RULEVLD and RSRCVLD attributes specified, this not a finding.

If any logonid with the SECURITY attribute does not have the RULEVLD and/or RSRCVLD attributes specified, this is a finding.

Fix Text: Configure Logonids with the SECURITY attribute to have the RULEVLD and RSRCVLD attributes specified.

If a logonid is granted the SECURITY privilege, it is mandatory that RULEVLD and RSRCVLD attributes will also be specified for the logonid.

Example:
SET LID
CHANGE logonid RULEVLD RSRCVLD

CCI: CCI-000366

Group ID (Vulid): V-223472
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223472r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000540
Rule Title: IBM z/OS LOGONIDs with the AUDIT or CONSULT attribute must be properly scoped.
Legacy ID: SV-106747
Legacy ID: V-97643

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 ACF Command Screen enter:
SET LID
LIST IF(AUDIT)

If all logonids with the attributes AUDIT and/or CONSULT also do not have the SCPLIST attribute specified properly according to job function and areas of responsibility, this is a finding.

NOTE: SCPLST attributes are not required for Logonids with the attributes AUDIT or CONSULT if the security ISSM/ISSO determines it requires ability to view the entire ACF2 environment. SCPLST attributes are not required for Auditors, Domain Level Security Admin Logonids, and BATCH Logonids that review the entire ACF2 environment to include GSO records, data set and resource rules, etc. or run audit reports.

Fix Text: Configure logonids with the AUDIT or CONSULT attributes are restricted by a SCPLIST attribute that restricts authority based on job function and area of responsibility.

The following user attributes allow viewing of the ACF2 databases for the purpose of inspecting users, data set access rules, and Infostorage records. When granted to a logonid, restrict the scope of the following attributes using an associated SCPLIST (scope list) record:

AUDIT
CONSULT

NOTE: SCPLST attributes are not required for Logonids with the attributes AUDIT or CONSULT if the security ISSM/ISSO determines it requires ability to view the entire ACF2 environment. SCPLST attributes are not required for Auditors, Domain Level Security Admin Logonids, and BATCH Logonids that review the entire ACF2 environment to include GSO records, data set and resource rules, etc. or run audit reports.

CCI: CCI-000366

Group ID (Vulid): V-223473
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223473r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000550
Rule Title: IBM z/OS LOGONID with the ACCTPRIV attribute must be restricted to the ISSO.
Legacy ID: SV-106749
Legacy ID: V-97645

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 ACF Command screen enter:
SET LID
LIST IF(ACCTPRIV)

If logonids with the ACCTPRIV attribute specified are not assigned to the security administrator, this is a finding.

Fix Text: Configure logonids with the ACCTPRIV attribute to be only reserved for use by the Security manager.

The ACCTPRIV attribute cannot be scoped, and will be restricted exclusively to a site security administrator:

Example:
SET LID
CHANGE logonid ACCTPRIV

CCI: CCI-000366

Group ID (Vulid): V-223474
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223474r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000560
Rule Title: IBM z/OS batch jobs with restricted ACF2 LOGONIDs must have the PGM(xxxxxxxx) and SUBAUTH attributes or the SOURCE(xxxxxxxx) attribute assigned to the corresponding LOGONIDs.
Legacy ID: V-97647
Legacy ID: SV-106751

Vulnerability Discussion: Activity under unusual conditions can indicate hostile activity. For example, what is normal activity during business hours can indicate hostile activity if it occurs during off hours.

Depending on mission needs and conditions, account usage restrictions based on conditions and circumstances may be critical to limit access to resources and data to comply with operational or mission access control requirements. Thus, the operating system must be configured to enforce the specific conditions or circumstances under which organization-defined accounts can be used (e.g., by restricting usage to certain days of the week, time of day, or specific durations of time).

Check Content:
From the ACF command screen enter:
SET LID
SET VERBOSE
LIST IF(RESTRICT)

If the logonids that are associated with batch jobs have the RESTRICT attribute, then the logonids must also have the PGM(xxxxxxxx) and SUBAUTH attributes, or the SOURCE(xxxxxxxx) attribute specified.

If all restricted logonids have the PGM(xxxxxxxx) and SUBAUTH attributes, and/or the SOURCE(xxxxxxxx) attribute, this is not a finding.

If the PGM(xxxxxxxx) and SUBAUTH attributes or the SOURCE(xxxxxxxx) attribute is not specified for any restricted logonids, this is a finding.

Fix Text: All batch jobs scheduled via an automation process will use the //*LOGONID xxxxxxxx card in the JCL stream to identify the userid. Use restricted logonids with the following parameter coded:

RESTRICT

One or both of the following will also be specified:

PGM(xxxxxxxx) and SUBAUTH
SOURCE(xxxxxxxx)

The use of default IDs prevents the identification of tasks with individual users as mandated by policy, and prevents adequate accountability. Default IDs for batch processing will not be used.

The use of USER= can also be used in the jobcard to identify the userid to be used for a job's processing.

CCI: CCI-000366

Group ID (Vulid): V-223475

Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223475r695416_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000570
Rule Title: CA-ACF2 RULEOPTS GSO record values must be set to the values specified.
Legacy ID: V-97649
Legacy ID: SV-106753

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 ACF Command enter:
SET CONTROL(GSO)
LIST RULEOPTS

If the following options are defined, this is not a finding.

NO$NOSORT
CENTRAL
CHANGE
DECOMP(AUDIT SECURITY) | DECOMP(AUDIT) | DECOMP(SECURITY)

The other RULEOPTS values should be assigned carefully as they affect the Rules and Infostorage databases.

Fix Text: Configure the GSO RULEOPTS record values to conform to the following requirements.

NO$NOSORT
CENTRAL
CHANGE
DECOMP(AUDIT SECURITY) | DECOMP(AUDIT) | DECOMP(SECURITY)

The other RULEOPTS values should be assigned carefully as they affect the Rules and Infostorage databases.

Example:
SET C(GSO)
INSERT RULEOPTS NO$NOSORT CENTRAL CHANGE NOCOMPDYN DECOMP(AUDIT SECURITY)

F ACF2,REFRESH(RULEOPTS)

CCI: CCI-000366

CCI: CCI-000368

Group ID (Vulid): V-223476
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223476r695413_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000580
Rule Title: The CA-ACF2 GSO OPTS record value must be properly specified.
Legacy ID: V-97651
Legacy ID: SV-106755

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 ACF Command enter:
SET CONTROL(GSO)
LIST OPTS

If the GSO OPTS record values conform to the following requirements, this is not a finding.

BLPLOG
NOCMDREC
CONSOLE(NOROLL)
CPUTIME(LOCAL)
DATE(MDY)
NODDB
DFTLID()
DFTSTC()
INFOLIST(none | AUDIT | SECURITY | SECURITY, AUDIT)
JOBCK
MAXVIO(10)
NOTIFY
RPTSCOPE

SHRDASD
STAMPSMF
STC
TAPEDSN
TEMPDSN
NOUADS
NOVTAMOPEN

Fix Text: Define the global options available to the system.

BLPLOG
NOCMDREC
CONSOLE(NOROLL)
CPUTIME(LOCAL)
DATE(MDY)
NODDB
DFTLID()
DFTSTC()
INFOLIST(none | AUDIT | SECURITY | SECURITY, AUDIT)
JOBCK
MAXVIO(10)
NOTIFY
RPTSCOPE
SHRDASD
STAMPSMF
STC
TAPEDSN
TEMPDSN
NOUADS
NOVTAMOPEN

Example:
SET C(GSO)
INSERT OPTS BLPLOG NOCMDREC CONSOLE(NOROLL) CPUTIME(LOCAL)
DATE(MDY) NODDB DFTLID() DFTSTC() INFOLIST(SECURITY, AUDIT) JOBCK
MAXVIO(10)
MODE(ABORT) NOTIFY RPTSCOPE SHRDASD STAMPSMF STC TAPEDSN TEMPDSN
NOUADS NOVTAMOPEN

F ACF2,REFRESH(OPTS)

CCI: CCI-000366

Group ID (Vulid): V-223477
Group Title: SRG-OS-000480-GPOS-00225
Rule ID: SV-223477r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000590
Rule Title: CA-ACF2 must prevent the use of dictionary words for passwords.
Legacy ID: V-97653
Legacy ID: SV-106757

Vulnerability Discussion: If the operating system allows the user to select passwords based on dictionary words, then this increases the chances of password compromise by increasing the opportunity for successful guesses and brute-force attacks.

Check Content:
From the ISPF Command Shell enter:
ACF to enter ACF2 Command shell
enter SHOW STATE

If "PSWDRSV = NO", this is a finding.

If "PSWDRSVW = NO", this is a finding.

SHOW PSwdopts

Reserved Words and Prefixes
APPL APR ASDF AUG BASIC
CADAM DEC DEMO FEB FOCUS
GAME IBM JAN JUL JUN
LOG MAR MAY NET NEW
NOV OCT PASS ROS SEP
SIGN SYS TEST TSO VALID
VTAM XXX 1234

Fix Text: Configure the GSO record to include PSWDRSV and PSWDRSVW.

CCI: CCI-000366

Group ID (Vulid): V-223478
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223478r928967_rule

Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000600
Rule Title: CA-ACF2 database must be on a separate physical volume from its backup and recovery data sets.
Legacy ID: V-97655
Legacy ID: SV-106759

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 ACF Command screen, enter:
SET CONTROL(GSO)
SHOW DDSN

Exexute the ISPF Data Set List Utility for each dataset listed to determine the volume.

If the ACF2 database is not located on the same volume as either its alternate or backup file, this is not a finding.

If the ACF2 database is collocated with either its alternate or backup, this is a finding.

Fix Text: Configure the placement of ACF2 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 ACF2 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 ACF2 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 ACF2 database should not also cause the loss of the ACF2 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 ACF2 database and its alternate or backup file.

CCI: CCI-000366

Group ID (Vulid): V-223479

Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223479r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000610
Rule Title: CA-ACF2 database must be backed up on a scheduled basis.
Legacy ID: V-97657
Legacy ID: SV-106761

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 ACF Command enter:
SET CONTROL(GSO)
SHOW SYSTEMS

If based on the information provided, it can be determined that the ESM database is being backed up on a regularly scheduled basis, this is not a finding.

If it cannot be determined that the ESM database is being backed up on a regularly scheduled basis, this is a finding.

Fix Text: Configure ACF2 GSO option to ensure that procedures are in place to back up all ACP files needed for recovery on a scheduled basis.

At a minimum, this means nightly backup of the ACP databases and of other critical security files (such as the ACP parameter file). More frequent backups (two or three times daily) will reduce the time necessary to effect recovery. The ISSO will verify that the backup job(s) run successfully.

CCI: CCI-000366

Group ID (Vulid): V-223480
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223480r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000620
Rule Title: ACF2 REFRESH attribute must be restricted to security administrators only.
Legacy ID: SV-106763
Legacy ID: V-97659

Vulnerability Discussion: Activity under unusual conditions can indicate hostile activity. For example, what is normal activity during business hours can indicate hostile activity if it occurs during off hours.

Depending on mission needs and conditions, account usage restrictions based on conditions and circumstances may be critical to limit access to resources and data to comply with operational or mission access control requirements. Thus, the operating system must be configured to enforce the specific conditions or circumstances under which organization-defined accounts can be used (e.g., by restricting usage to certain days of the week, time of day, or specific durations of time).

Check Content:
From the ACF Command screen enter:
SET LID
LIST IF(REFRESH)

If logonids exist with the REFRESH attribute not assigned to a site security administrator, this is a finding.

Fix Text: Define any logonid with the REFRESH attribute to be assigned to a site security administrator only.

Example:
SET LID
CHANGE logonid REFRESH

CCI: CCI-000366

Group ID (Vulid): V-223481
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223481r695419_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000630
Rule Title: ACF2 maintenance LOGONIDs must have corresponding GSO MAINT records.
Legacy ID: SV-106765
Legacy ID: V-97661

Vulnerability Discussion: Activity under unusual conditions can indicate hostile activity. For example, what is normal activity during business hours can indicate hostile activity if it occurs during off hours.

Depending on mission needs and conditions, account usage restrictions based on conditions and circumstances may be critical to limit access to resources and data to comply with operational or mission access control requirements. Thus, the operating system must be configured to enforce the specific conditions or circumstances under which organization-defined accounts can be used (e.g., by restricting usage to certain days of the week, time of day, or specific durations of time).

Check Content:
From the ACF Command screen enter:
SET LID
LIST IF(MAINT)

SET CONTROL(GSO)
LIST LIKE(MAINT-)

If every maintenance logonid has a corresponding GSO MAINT record, this is not a finding.

Fix Text: Ensure that an associated GSO maintenance record exists for each special user logonid identifying the program(s) that it is permitted to access and the library where the program(s) resides.

Define associated GSO MAINT record for each special user logonid, identifying the program(s) that it is permitted to access and the library where the program(s) resides.

Every maintenance logonid has a corresponding GSO MAINT record.

Example:

SET C(GSO)
INSERT MAINT.DFSMSHSM LIBRARY(SYS1.LINKLIB) LID(HSMDFDSS)
PGM(ADRDSSU)

F ACF2,REFRESH(MAINT)

CCI: CCI-000366

Group ID (Vulid): V-223482
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223482r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000640
Rule Title: ACF2 LOGONIDs with the NON-CNCL attribute specified in the associated LOGONID record must be listed as trusted and must be specifically approved.

Legacy ID: SV-106767
Legacy ID: V-97663

Vulnerability Discussion: Activity under unusual conditions can indicate hostile activity. For example, what is normal activity during business hours can indicate hostile activity if it occurs during off hours.

Depending on mission needs and conditions, account usage restrictions based on conditions and circumstances may be critical to limit access to resources and data to comply with operational or mission access control requirements. Thus, the operating system must be configured to enforce the specific conditions or circumstances under which organization-defined accounts can be used (e.g., by restricting usage to certain days of the week, time of day, or specific durations of time).

Check Content:
From the ACF command screen enter:
SET LID
SET VERBOSE
LIST IF(NON-CNCL)

If only logonids associated with trusted STCs have the NON-CNCL attribute specified, this is not a finding.

TRUSTED STCs:
STCs that are listed as z/OS started tasks and address spaces in the IBM z/OS MVS Initialization and Tuning Reference.

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 all LOGONIDs with the NON-CNCL attribute. Ensure that only STCs in the trusted list 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.

These STCs will be given the following attribute to facilitate access while logging any accesses they would not ordinarily be granted by the access rule sets:

NON-CNCL

Example:
SET LID
CHANGE logonid STC NON-CNCL

CCI: CCI-000366

Group ID (Vulid): V-223483
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223483r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000650
Rule Title: ACF2 LOGONIDs with the ACCOUNT, LEADER, or SECURITY attribute must be properly scoped.
Legacy ID: SV-106769
Legacy ID: V-97665

Vulnerability Discussion: Activity under unusual conditions can indicate hostile activity. For example, what is normal activity during business hours can indicate hostile activity if it occurs

during off hours.

Depending on mission needs and conditions, account usage restrictions based on conditions and circumstances may be critical to limit access to resources and data to comply with operational or mission access control requirements. Thus, the operating system must be configured to enforce the specific conditions or circumstances under which organization-defined accounts can be used (e.g., by restricting usage to certain days of the week, time of day, or specific durations of time).

Check Content:
From the ACF command screen enter:
SET LID
LIST IF(ACCOUNT)
LIST IF(LEADER)
LIST IF(SECURITY)

Review all logonids for specific groups with the attributes ACCOUNT, LEADER, or SECURITY.

If each has the SCPLIST attribute specified properly according to job function and areas of responsibility, this is not a finding.

NOTE: SCPLST attributes are not required for Domain Level Security Admin Logonids and BATCH Logonids that administer and modify the entire ACF2 environment to include GSO records, data set and resource rules, etc. or run audit reports.

Fix Text: The following user attributes allow update of the ACF2 databases for administering users, data set access rules, and Infostorage records. When granted to a logonid, restrict the scope of the following attributes using an associated SCPLIST (scope list) record:

ACCOUNT
LEADER
SECURITY

NOTE: SCPLST attributes are not required for Domain Level Security Admin Logonids and BATCH Logonids that administer and modify the entire ACF2 environment to include GSO records, data set and resource rules, etc. or run audit reports.

CCI: CCI-000366

Group ID (Vulid): V-223484
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223484r836695_rule
Severity: CAT II

Rule Version (STIG-ID): ACF2-ES-000660
Rule Title: ACF2 LOGONIDs associated with started tasks that have the MUSASS attribute and the requirement to submit jobs on behalf of its users must have the JOBFROM attribute as required.
Legacy ID: SV-106771
Legacy ID: V-97667

Vulnerability Discussion: Activity under unusual conditions can indicate hostile activity. For example, what is normal activity during business hours can indicate hostile activity if it occurs during off hours.

Depending on mission needs and conditions, account usage restrictions based on conditions and circumstances may be critical to limit access to resources and data to comply with operational or mission access control requirements. Thus, the operating system must be configured to enforce the specific conditions or circumstances under which organization-defined accounts can be used (e.g., by restricting usage to certain days of the week, time of day, or specific durations of time).

Check Content:
From the ACF command screen enter:
SET LID
SET VERBOSE
LIst IF(MUSASS & STC)

If any started task logonid that has the MUSASS attribute and the requirement to submit jobs on behalf of its users does not have the JOBFROM attribute, this is a finding.

Fix Text: Ensure that if MUSASS has the requirement to submit jobs on behalf of its users, the STC logonid has the JOBFROM attribute specified.

If the MUSASS has the requirement to submit jobs on behalf of its users, the STC logonid will also have the following attribute:

JOBFROM

Example:

SET LID
CHANGE logonid STC JOBFROM

CCI: CCI-000366

Group ID (Vulid): V-223485

Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223485r877342_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000670
Rule Title: IBM z/OS Started Tasks must be properly identified and defined to ACF2.
Legacy ID: V-97669
Legacy ID: SV-106773

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.

From the ACF command screen enter:
SET LID
SET VERBOSE
LIST IF(STC)

If all logonids identified as started tasks have the STC attribute specified, this is not a finding.

Fix Text: All started tasks will be assigned an individual logonid. The logonid for a Started Task Control (STC) will be granted the minimum privileges necessary for the STC to function. In addition to the default LID field settings, all STC logonids will have the following field setting:

STC

Example:
SET LID
INSERT logonid STC

CCI: CCI-000764

Group ID (Vulid): V-223486
Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223486r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000680
Rule Title: ACF2 emergency LOGONIDS with the REFRESH attribute must have the SUSPEND attribute specified.
Legacy ID: V-97671
Legacy ID: SV-106775

Vulnerability Discussion: Activity under unusual conditions can indicate hostile activity. For example, what is normal activity during business hours can indicate hostile activity if it occurs during off hours.

Depending on mission needs and conditions, account usage restrictions based on conditions and circumstances may be critical to limit access to resources and data to comply with operational or mission access control requirements. Thus, the operating system must be configured to enforce the specific conditions or circumstances under which organization-defined accounts can be used (e.g., by restricting usage to certain days of the week, time of day, or specific durations of time).

Check Content:
From the ACF Command screen enter:
SET LID
LIST IF(REFRESH)

If the logonid is an emergency logonid and the REFRESH attribute is not in SUSPEND status, this is a finding.

Fix Text: The emergency logonids with the REFRESH attribute must be in SUSPEND status unless actually in use.

Example:
SET LID
CHANGE logonid SUSPEND

CCI: CCI-000366

Group ID (Vulid): V-223487
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223487r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000690
Rule Title: ACF2 BACKUP GSO record must be defined with a TIME value specifies greater than 00 unless the database is shared and backed up on another system.

Legacy ID: V-97673
Legacy ID: SV-106777

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 ACF command screen enter:
SET CONTROL(GSO)
LIST LIKE(BACKUP-)

If the GSO BACKUP record values conform to the following requirements, this is not a finding.

Example:
CPUID() PRISPACE(5) SECSPACE(5) STRING(S ACFBKUP) TIME(00:01) WORKUNIT(VIO)

If there is any deviation from the above requirements in the GSO BACKUP record values, this is a finding.

Fix Text: Configure the BACKUP GSO value to specify a time field and Time(00:00) is not specified unless the database is shared and backed up on another system.

CPUID() PRISPACE(5) SECSPACE(5) STRING(S ACFBKUP) TIME(00:01) WORKUNIT(VIO)

Example:
SET C(GSO)
INSERT BACKUP CPUID() PRISPACE(5) SECSPACE(5) STRING(S ACFBKUP) TIME(00:01) WORKUNIT(VIO)

F ACF2,REFRESH(BACKUP)

CCI: CCI-000366

CCI: CCI-000537

Group ID (Vulid): V-223488
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223488r533198_rule
Severity: CAT III
Rule Version (STIG-ID): ACF2-ES-000700
Rule Title: ACF2 APPLDEF GSO record if used must have supporting documentation indicating the reason it was used.
Legacy ID: V-97675
Legacy ID: SV-106779

Vulnerability Discussion: Failure to restrict network connectivity only to authorized systems permits inbound connections from malicious systems. It also permits outbound connections that may facilitate exfiltration of DoD data.

Check Content:
From the ACF Command screen enter:
SET CONTROL(GSO)
LIST LIKE(APPLDEF-)

If the GSO APPLDEF record does not exist, this is not a finding.

If the GSO APPLDEF record does exist and no supporting documentation is available, this is a finding.

Fix Text: For any APPLDEF GSO record used, it must have supporting documentation indicating the reason it was used.

The APPLDEF record is optional.

CCI: CCI-000366

CCI: CCI-000368

Group ID (Vulid): V-223489
Group Title: SRG-OS-000368-GPOS-00154

Rule ID: SV-223489r853531_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000710
Rule Title: ACF2 MAINT GSO record value if specified must be restricted to production storage management user.
Legacy ID: V-97677
Legacy ID: SV-106781

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 ACF Command screen enter:
SET CONTROL(GSO)
LIST LIKE(MAINT-)

If the GSO MAINT record values conform to the following requirements, this is not a finding.

Specifies the logonid, program, and library combinations used for system maintenance functions.
NOTE: For logonids that match environments described in records, no SMF logging records will be created.
NOTE: Entries will be restricted to production storage management user accounts and programs.

If there is any deviation from the above requirements in the GSO MAINT record values, this is a finding.

Fix Text: Configure the MAINT GSO value to be specified as restricted to production storage management user accounts and programs.

Specifies the logonid, program, and library combinations used for system maintenance functions.
NOTE: For logonids that match environments described in records, no SMF logging records will be created.

NOTE: Entries will be restricted to production storage management user accounts and programs.

CCI: CCI-001764

Group ID (Vulid): V-223490
Group Title: SRG-OS-000368-GPOS-00154
Rule ID: SV-223490r853532_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000720
Rule Title: ACF2 LINKLST GSO record if specified must only contains trusted system data sets.
Legacy ID: V-97679
Legacy ID: SV-106783

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 ACF Command screen enter:
SET CONTROL(GSO)
LIST LINKLST

If the GSO LINKLST record values conform to the following requirements, this is not a finding.

Specifies one or more partitioned data sets considered part of the system link (SYS1.LINKLIB) during data set access validation. Only trusted system data sets will be listed. Application libraries will never be included.

Example:

LIBRARY(SYS1.LINKLIB SYS2A.FDR.LOADLIB)

If there is any deviation from the above requirements in the GSO LINKLST record values, this is a finding.

Fix Text: Configure the LINKLIST GSO value if specified only contains trusted system data sets.

Specifies one or more partitioned data sets considered part of the system link (SYS1.LINKLIB) during data set access validation.

Only trusted system data sets will be listed. Application libraries will never be included.

Example:
SET C(GSO)
INSERT LINKLST LIBRARY(SYS1.LINKLIB SYS2A.FDR.LOADLIB)

F ACF2,REFRESH(LINKLST)

CCI: CCI-001764

Group ID (Vulid): V-223491
Group Title: SRG-OS-000096-GPOS-00050
Rule ID: SV-223491r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000730
Rule Title: IBM z/OS must properly protect MCS console userid(s).
Legacy ID: SV-106785
Legacy ID: V-97681

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 the correct CONSOLxx member.

Examine the CONSOLxx member.

Verify that the MCS console logonids are properly restricted.

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

Each console defined in the currently active CONSOLxx parmlib member is associated with a valid ACF2 logonid.

Each console logonid has no special privileges and/or attributes (e.g., ACCOUNT, SECURITY, etc.).

Each console logonid has no accesses to interactive online facilities (e.g., TSO, CICS, etc., excluding VTAM SMCS consoles).

Each console logonid 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 logonids may be given with SERVICE(READ) to MVS.CONTROL, MVS.DISPLAY, MVS.MONITOR, and MVS.STOPMN OPERCMDS resources.

NOTE: Execute the JCL in CNTL(ACFRPTRX) using the ACF2 console userids in the LID statements in the SYSIN input. This report lists all occurrences of these userids within the ACF2 database, including data set and resource access lists.

Fix Text: Define all consoles identified in the currently active CONSOLxx parmlib member in EXAM.RPT(PARMLIB) to be defined to the ESM.

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

Each console defined in the currently active CONSOLxx parmlib member is associated with a valid ACF2 logonid.

Each console logonid has no special privileges and/or attributes (e.g., ACCOUNT, SECURITY, etc., excluding VTAM SMCS consoles).

Each console logonid has no accesses to interactive online facilities (e.g., TSO, CICS, etc.).

Each console logonid 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 logonids may be given with SERVICE(READ) to MVS.CONTROL, MVS.DISPLAY, MVS.MONITOR, and MVS.STOPMN OPERCMDS resources.

NOTE: If LOGON(AUTO) is specified in the currently active CONSOLxx parmlib member, additional access may be required. Permissions for the console logonids may be given with SERVICE(READ) to MVS.CONTROL, MVS.DISPLAY, MVS.MONITOR, and MVS.STOPMN OPERCMDS resources.

Example:
INSERT MVAC20 NAME(MVA CONSOLE C20) PASSWORD(xxxxxxxx)

$KEY(MVS) TYPE(OPR)
MCSOPER.- UID(MVAC20) SERVICE(READ) ALLOW
CONTROL.- UID(MVAC20) SERVICE(READ) ALLOW DATA(FOR LOGON(AUTO))
MONITOR.- UID(MVAC20) SERVICE(READ) ALLOW DATA(FOR LOGON(AUTO))
STOPMN.- UID(MVAC20) SERVICE(READ) ALLOW DATA(FOR LOGON(AUTO))
DISPLAY.- UID(*) SERVICE(READ) ALLOW
- UID(*) PREVENT

SET R(OPR)
COMPILE ' ACF2.MVA.OPR(MVS)' STORE

F ACF2,REBUILD(OPR)

$KEY(consname) TYPE(CON)
UID(MVAC20) SERVICE(READ) ALLOW

SET R(CON)
COMPILE ' ACF2.MVA.CON(consname)' STORE

F ACF2,REBUILD(CON)

CCI: CCI-000382

Group ID (Vulid): V-223492

Group Title: SRG-OS-000096-GPOS-00050
Rule ID: SV-223492r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000740
Rule Title: ACF2 BLPPGM GSO record must not be defined.
Legacy ID: SV-106787
Legacy ID: V-97683

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 ISPF Command Shell enter:
ACF
SET CONTROL(GSO)
LIST BLPPGM

If the BLPPGM record is defined, this is a finding.

Fix Text: The BLPPGM GSO value indicates that ACF2 does not control the programs authorized to use tape bypass label processing (BLP).

Delete the BLPPGM from GSO options.

CCI: CCI-000382

Group ID (Vulid): V-223493
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223493r695420_rule

Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000750
Rule Title: IBM z/OS UID(0) must be properly assigned.
Legacy ID: SV-106789
Legacy ID: V-97685

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 ACF command screen enter:
SET PROFILE(USER) DIVISION(OMVS)
SET VERBOSE
LIST LIKE(-)

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: Assure that UID(0) is defined 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-223494
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223494r836650_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000760
Rule Title: IBM z/OS user account for the UNIX kernel (OMVS) must be properly defined to the security database.
Legacy ID: SV-106791
Legacy ID: V-97687

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:

ACF
SET LID
SET VERBOSE
LIST OMVS SECTION(ALL) PROFILE(OMVS)

If OMVS 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"

If OMVS is not defined as specified in above, this is a finding.

Fix Text: Define the OMVS (IBM default name for USS Kernel), 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-223495
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223495r861168_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000770
Rule Title: IBM z/OS user account for the UNIX (RMFGAT) must be properly defined.
Legacy ID: V-97689
Legacy ID: SV-106793

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 the ISPF Command Shell enter:
ACF
SET LID
SET VERBOSE
LIST RMFGAT SECTION(ALL) PROFILE(OMVS)

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 the RMFGAT user account 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-223496
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223496r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000780
Rule Title: ACF2 LOGONIDs must be defined with the required fields completed.
Legacy ID: V-97691
Legacy ID: SV-106795

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 an ACF Command Screen enter:
SET LID
LIST *

If the below listed fields are complete for all logonids, this is not a finding.

NAME User's name
UID-String All fields defined in the ACFFDR @UID macro

NOTE: A completed NAME field that can either be traced back to a current DD Form 2875 or a Vendor Requirement (example: A Started Task).

NOTE: A user may be required to have more than one logonid but users must not share userids.

Fix Text: Define every user to ACF2 with a unique userid. (ACF2 calls this a logonid.) To ACF2, a user is an individual, a started task, or a batch job.

Every user will be fully identified within ACF2. Complete the following fields for every logonid:

NAME - User's name
UID-String - All fields defined in the ACFFDR @UID macro

All fields that comprise the standard UID string will be filled out for each user as a logonid is added.

Example:
SET LID
INSERT logonid UID(uid string) NAME(user name)

CCI: CCI-000764

Group ID (Vulid): V-223497
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223497r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000790
Rule Title: CA-ACF2 defined user accounts must uniquely identify system users.
Legacy ID: V-97693
Legacy ID: SV-106797

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.

Satisfies: SRG-OS-000104-GPOS-00051, 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: Userids should be able to be traced back to a current DD Form 2875 or a Vendor Requirement (example: A Started Task).

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-000764

CCI: CCI-000804

CCI: CCI-000877

Group ID (Vulid): V-223498
Group Title: SRG-OS-000118-GPOS-00060
Rule ID: SV-223498r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000800
Rule Title: CA-ACF2 userids found inactive for more than 35 days must be suspended.
Legacy ID: V-97695
Legacy ID: SV-106799

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:
ACF

If every user shows an ACC-DATE=mm/dd/yy 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 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-223499
Group Title: SRG-OS-000266-GPOS-00101
Rule ID: SV-223499r695422_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000810
Rule Title: CA-ACF2 PWPHRASE GSO record must be properly defined.
Legacy ID: V-97697
Legacy ID: SV-106801

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 in determining 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.

Special characters are those characters that are not alphanumeric. Examples include: ~ ! @ # $ % ^ *.

Check Content:
From the ISPF Command Screen enter:
ACF
SET CONTROL(GSO)
LIST PWPHRASE
If the following options are in effect, this is not a finding.

If any of the options deviate from the following, this is a finding.

The GSO PWPHRASE record will conform to the following requirements.

ALPHA(1 or greater)
HISTORY(10-32)
MAXDAYS(1-60)
MINDAYS(1)
MINLEN(15-100)
NUMERIC(1 or greater)
SPECIAL(1 or greater)

SPECLIST(character list)
WARNDAYS(1-10)

Note: The SPECLIST special characters will be specified at a minimum. Characters will conform to the allowable list defined in CA ACF2 for z/OS Administration Guide.

Fix Text: Configure the PWPHRASE GSO values to be set to the values specified.

Ensure the GSO PWPHRASE record values conform to the following requirements:

ALPHA(1 or greater)
HISTORY(10-32)
MAXDAYS(1-60)
MINDAYS(1)
MINLEN(15-100)
NUMERIC(1 or greater)
SPECIAL(1 or greater)
SPECLIST(character list)
WARNDAYS(1-10)

Note: The SPECLIST special characters will be specified at a minimum. Characters will conform to the allowable list defined in CA ACF2 for z/OS Administration Guide.

Example:
SET C(GSO)
INSERT PWPHRASE NOALLOW ALPHA(1) HISTORY(10) MAXDAYS(60) MINDAYS(1) MINLEN(15) NUMERIC(1) SPECIAL(1) SPECLIST(& * =) WARNDAYS(10)

F ACF2,REFRESH(PWPHRASE)

CCI: CCI-001619

Group ID (Vulid): V-223500
Group Title: SRG-OS-000266-GPOS-00101
Rule ID: SV-223500r695424_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000820
Rule Title: CA-ACF2 must enforce password complexity by requiring that at least one special character be used.
Legacy ID: V-97699
Legacy ID: SV-106803

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 in determining 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.

Special characters are those characters that are not alphanumeric. Examples include: ~ ! @ # $ % ^ *.

Check Content:
From an ACF command screen enter:
SET CONTROL(GSO)
LIST PSWD

If PSWDPLST is coded as defined in CA ACF2 for z/OS Administration Guide, this is not a finding.

Fix Text: Configure Password option PSWDPLST as defined in CA ACF2 for z/OS Administration Guide.

CCI: CCI-001619

Group ID (Vulid): V-223501
Group Title: SRG-OS-000069-GPOS-00037
Rule ID: SV-223501r695426_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000840
Rule Title: ACF2 PSWD GSO record value must be set to require at least one upper-case character be used.
Legacy ID: SV-106807
Legacy ID: V-97703

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.

Check Content:
From the ISPF Command Shell enter:

ACF to enter ACF2 Command shell
enter
SET CONTROL(GSO)
LIST PSWD
If NOPSWDUC is listed, this is a finding.

Fix Text: Configure the GSO option "PSWDUC" to "YES".

CCI: CCI-000192

Group ID (Vulid): V-223502
Group Title: SRG-OS-000071-GPOS-00039
Rule ID: SV-223502r695429_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000850
Rule Title: ACF2 PSWD GSO record value must be set to require at least one numeric character be used.
Legacy ID: SV-106809
Legacy ID: V-97705

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.

Check Content:
From an ACF command screen enter:
SET CONTROL(GSO)
LIST PSWD

If "PSWDALPH" is coded, this is not a finding.

Fix Text: Configure the Password options to include "PSWDALPH".

CCI: CCI-000194

Group ID (Vulid): V-223503
Group Title: SRG-OS-000070-GPOS-00038
Rule ID: SV-223503r861169_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000860
Rule Title: ACF2 PSWD GSO record value must be set to require at least one lower-case character be used.
Legacy ID: SV-106811
Legacy ID: V-97707

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.

Check Content:
From the ISPF Command Shell enter:
ACF to enter ACF2 Command shell
enter SET CONTROL(GSO)

LIST PSWD

If "NOPSWDLC" is listed, this is a finding.

Fix Text: Configure the GSO option "PSWDLC" to "YES".

CCI: CCI-000193

Group ID (Vulid): V-223504
Group Title: SRG-OS-000072-GPOS-00040
Rule ID: SV-223504r695433_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000870
Rule Title: ACF2 PSWD GSO record value must be set to require the change of at least 50% of the total number of characters when passwords are changed.
Legacy ID: SV-106813
Legacy ID: V-97709

Vulnerability Discussion: If the operating system allows the user to consecutively reuse extensive portions of passwords, this increases the chances of password compromise by increasing the window of opportunity for attempts at guessing and brute-force attacks.

The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. In other words, characters may be the same within the two passwords; however, the positions of the like characters must be different.

If the password length is an odd number then number of changed characters must be rounded up. For example, a password length of 15 characters must require the change of at least 8 characters.

Check Content:
From an ACF command screen enter:
SET CONTROL(GSO)
LIST PSWD

If "PSWDSIM" is set to "4", this is not a finding.

Fix Text: Configure the Password option "PSWDSIM" to "4".

CCI: CCI-000195

Group ID (Vulid): V-223505
Group Title: SRG-OS-000073-GPOS-00041
Rule ID: SV-223505r877397_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000880
Rule Title: ACF2 must use NIST FIPS-validated cryptography to protect passwords in the security database.
Legacy ID: SV-106817
Legacy ID: V-97713

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 an ACF command screen enter:
SET CONTROL(GSO)
LIST PSWD

If the "GSO PSWD" record option "PSWDENCT" is set to "XDES" or null, this is a finding.

SET MSYSID(-)

LIST PSWD

For CA-ACF2 R16 and above:

If option "NOONEPWALG" is specified, and there is no transition plan with a definite completion date filed with the ISSM, 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 as specified below:

Configure the "GSO PSWD" record option "PSWDENCT" to "AES1".

For CA-ACF2 Release16 and above:

Configure "GSO PSWD" record option "PSWDENCT" to "AES1" or "AES2".

Configure the "GSO PSWD" to "ONEPWALG".

Note: If you are using VM Database Synchronization you cannot use "ONEPWALG". VM does not support the AES algorithms.

Develop a transition plan with a definite completion date for z/VM; file with the ISSM.

If all systems that are sharing the logonid or infostorage databases are not running with the same "PSWDENCT" value you cannot use "ONEPWALG".

Develop a transition plan that contains a definite completion date to migrate all logonid and infostorage databases to one "PSWDENCT" value; file with the ISSM.

Consult the CA-ACF2 administration guide for converting to "AES1" or "AES2" and using "ONEPWALG".

CCI: CCI-000196

CCI: CCI-000197

Group ID (Vulid): V-223506
Group Title: SRG-OS-000076-GPOS-00044
Rule ID: SV-223506r695437_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000890
Rule Title: ACF2 PSWD GSO record value must be set to require a 60-day maximum password lifetime restriction.
Legacy ID: V-97715
Legacy ID: SV-106819

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 an ACF command screen enter:
SET CONTROL(GSO)
LIST PSWD

If "PSWDMAX" is set to "60", this is not a finding.

Fix Text: Configure Password option "PSWDMAX" to "60" days.

CCI: CCI-000199

Group ID (Vulid): V-223507
Group Title: SRG-OS-000075-GPOS-00043
Rule ID: SV-223507r695439_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000900
Rule Title: ACF2 PSWD GSO record value must be set to require 24 hours/1 day as the minimum password lifetime.
Legacy ID: V-97717
Legacy ID: SV-106821

Vulnerability Discussion: Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, then the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Check Content:
From an ACF command screen enter:
SET CONTROL(GSO)
LIST PSWD

If "PSWDMIN" is set "1", this is not a finding.

Fix Text: Configure Password option "PSWDMIN" to minimum of "1" day.

CCI: CCI-000198

Group ID (Vulid): V-223508
Group Title: SRG-OS-000077-GPOS-00045
Rule ID: SV-223508r695441_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000910
Rule Title: ACF2 PSWD GSO record value must be set to prohibit password reuse for a minimum of five generations or more.
Legacy ID: V-97719
Legacy ID: SV-106823

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 an ACF command screen enter:
SET CONTROL(GSO)
LIST PSWD

If "PSWDXHIST" is not specified, this is a finding.

If "PSWDXHIST#" is set to "5" or greater, this is not a finding

Fix Text: Configure Password option "PSWXHST" is coded and "PSWXHST#" is "5" or greater.

CCI: CCI-000200

Group ID (Vulid): V-223509
Group Title: SRG-OS-000079-GPOS-00047
Rule ID: SV-223509r695443_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000920
Rule Title: ACF2 TSOTWX GSO record values must be set to obliterate the logon password on TWX devices.
Legacy ID: V-97721
Legacy ID: SV-106825

Vulnerability Discussion: To prevent the compromise of authentication information, such as passwords during the authentication process, the feedback from the operating system must not provide any information allowing an unauthorized user to compromise the authentication mechanism.

Obfuscation of user-provided information that is typed into the system is a method used when addressing this risk.

Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.

Check Content:
From the ISPF Command Shell enter:
ACF <enter>
SET CONTROL(GSO)
LIST TSOTWX

If the GSO TSOTWX record values conform to the following requirements, this is not a finding.

CR(15)
IDLE(17)
LENGTH(8)
M1(X)

M2(N)
M3(Z)
M4(M)
STRING()

Fix Text: Define a cross out mask to obliterate the logon password on TWX devices.

CR(15)
IDLE(17)
LENGTH(8)
M1(X)
M2(N)
M3(Z)
M4(M)
STRING()

Example:
SET C(GSO)
INSERT TSOTWX CR(15) IDLE(17) LENGTH(8) M1(X) M2(N) M3(Z) M4(M) STRING()

F ACF2,REFRESH(TSOTWX)

CCI: CCI-000206

Group ID (Vulid): V-223510
Group Title: SRG-OS-000079-GPOS-00047
Rule ID: SV-223510r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000930
Rule Title: ACF2 TSOCRT GSO record values must be set to obliterate the logon to ASCII CRT devices.
Legacy ID: V-97723
Legacy ID: SV-106827

Vulnerability Discussion: To prevent the compromise of authentication information, such as passwords during the authentication process, the feedback from the operating system must not provide any information allowing an unauthorized user to compromise the authentication mechanism.

Obfuscation of user-provided information that is typed into the system is a method used when addressing this risk.

Displaying asterisks when a user types in a password is an example of obscuring feedback of

authentication information.

Check Content:
From the ISPF Command Shell enter:
ACF
SET CONTROL(GSO) <enter>
LIST TSOCRT

If the GSO TSOCRT record values conform to the following requirements, this is not a finding.

STRING(A12FA11C1A270C0D)

Fix Text: Define a clear string used to obliterate the logon to ASCII CRT devices.

STRING(A12FA11C1A270C0D)

Example:
SET C(GSO)
INSERT TSOCRT STRING(A12FA11C1A270C0D)

F ACF2,REFRESH(TSOCRT)

CCI: CCI-000206

Group ID (Vulid): V-223511
Group Title: SRG-OS-000079-GPOS-00047
Rule ID: SV-223511r695445_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000940
Rule Title: ACF2 TSO2741 GSO record values must be set to obliterate the logon password on 2741 devices.
Legacy ID: SV-106829
Legacy ID: V-97725

Vulnerability Discussion: To prevent the compromise of authentication information, such as passwords during the authentication process, the feedback from the operating system must not provide any information allowing an unauthorized user to compromise the authentication mechanism.

Check Content:
From the ISPF Command Shell enter:

ACF <enter>
SET CONTROL(GSO)
LIST TSO2741

If the GSO TSO2741 record values conform to the following requirements, this is not a finding.

BS(16)
LENGTH(8)
M1(X)
M2(N)
M3(Z)
M4(M)
STRING()

Fix Text: Define a cross out string used to obliterate the logon password on 2741 devices.

Ensure the GSO TSO2741 record values conform to the following requirements.

BS(16)
LENGTH(8)
M1(X)
M2(N)
M3(Z)
M4(M)
STRING()

Example:
SET C(GSO)
INSERT TSO2741 BS(16) LENGTH(8) M1(X) M2(N) M3(Z) M4(M) STRING()

F ACF2,REFRESH(TSO2741)

CCI: CCI-000206

Group ID (Vulid): V-223512
Group Title: SRG-OS-000185-GPOS-00079
Rule ID: SV-223512r695447_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000950
Rule Title: ACF2 SECVOLS GSO record value must be set to VOLMASK(). Any local changes are justified and documented with the ISSO.
Legacy ID: V-97727
Legacy ID: SV-106831

Vulnerability Discussion: The SECVOLS record defines the DASD and tape volumes for which CA-ACF2 provides volume-level protection. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive and tape drive, when used for backups) within an operating system.

This requirement addresses protection of user-generated data, as well as operating system-specific configuration data. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate, in accordance with the security category and/or classification of the information.

Check Content:
From an ACF command screen enter:
SET CONTROL(GSO)
LIST SECVOLS

If the GSO SECVOLS record values conform to the following requirements, this is not a finding.

VOLMASK()

NOTE: Local changes will be documented in writing with supporting documentation.

If there is any deviation from the above requirements in the GSO SECVOLS record values, this is a finding.

Fix Text: Define the GSO SECVOLS record values to conform to the following requirements.

VOLMASK()

Example:
SET C(GSO)
INSERT SECVOLS VOLMASK()

F ACF2,REFRESH(SECVOLS)

CCI: CCI-000368

CCI: CCI-001199

Group ID (Vulid): V-223513
Group Title: SRG-OS-000185-GPOS-00079
Rule ID: SV-223513r864502_rule

Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000960
Rule Title: ACF2 RESVOLS GSO record value must be set to Volmask(-). Any other setting requires documentation justifying the change.
Legacy ID: SV-106835
Legacy ID: V-97731

Vulnerability Discussion: The RESVOLS record defines DASD and mass storage volumes for which CA ACF2 is to provide protection at the data set name level.
Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive and tape drive, when used for backups) within an operating system.

This requirement addresses protection of user-generated data, as well as operating system-specific configuration data. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate, in accordance with the security category and/or classification of the information.

Check Content:
From an ACF command screen, enter:
SET CONTROL(GSO)
LIST RESVOLS

If the GSO RESVOLS record values conform to the following requirements, this is not a finding.

VOLMASK(-)

NOTE: Local changes will be documented in writing with supporting documentation.

If there is any deviation from the above requirements in the GSO RESVOLS record values, this is a finding.

Fix Text: Define the GSO RESVOLS record values to conform to the following requirements.

VOLMASK(-)

Example:
SET C(GSO)
INSERT RESVOLS VOLMASK(-)

F ACF2,REFRESH(SECVOLS)

CCI: CCI-000368

CCI: CCI-001199

Group ID (Vulid): V-223514
Group Title: SRG-OS-000134-GPOS-00068
Rule ID: SV-223514r918612_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-ES-000970
Rule Title: ACF2 security data sets and/or databases must be properly protected.
Legacy ID: SV-106837
Legacy ID: V-97733

Vulnerability Discussion: An isolation boundary provides access control and protects the integrity of the hardware, software, and firmware that perform security functions.

Security functions are 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. Operating systems implement code separation (i.e., separation of security functions from nonsecurity functions) in a number of ways, including through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that serve to protect the code on disk and address space protections that protect executing code.

Developers and implementers can increase the assurance in security functions by employing well-defined security policy models; structured, disciplined, and rigorous hardware and software development techniques; and sound system/security engineering principles. Implementation may include isolation of memory space and libraries. Operating systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities.

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

Check Content:
Determine all associated ACF2 security data sets and/or databases.

If the ACF2 data set rules for ACF2 security data sets and/or databases restrict READ access to auditors and DASD batch, this is not a finding.

If the ACF2 data set rules for ACF2 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 ACP maintenance, this is not a finding.

If all (i.e., failures and successes) data set access authorities (i.e., READ, WRITE, ALLOCATE, and CONTROL) for ACP security data sets and/or databases are logged, this is not a finding.

Fix Text: Configure ACF2 READ and/or greater access rules for ACF2 files and/or databases as limited to system programmers and/or security personnel, and/or batch jobs that perform ACP maintenance.

READ access can be given to auditors and DASD batch. All accesses to ACP files and/or databases are logged.

CCI: CCI-000213

CCI: CCI-001084

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223515
Group Title: SRG-OS-000138-GPOS-00069
Rule ID: SV-223515r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000980
Rule Title: ACF2 AUTOERAS GSO record value must be set to indicate that ACF2 is controlling the automatic physical erasure of VSAM or non VSAM data sets.
Legacy ID: SV-106839
Legacy ID: V-97735

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 an ACF Command screen enter:
SET CONTROL(GSO)
LIST AUTOERAS

If the GSO AUTOERAS record values conform to the following requirements, this is not a finding.

All Systems: NON-VSAM VSAM VOLS(-)

Fix Text: Configure the AUTOERASE GSO value to indicate that ACF2 is controlling the automatic physical erasure of VSAM or non VSAM data sets.

Example:
SET C(GSO)
INSERT AUTOERAS NON-VSAM VSAM VOLS(-)

F ACF2,REFRESH(AUTOERAS)

CCI: CCI-001090

Group ID (Vulid): V-252705
Group Title: SRG-OS-000481-GPOS-00481
Rule ID: SV-252705r916433_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-ES-000990
Rule Title: The operating system must enforce a minimum 8-character password length.
Legacy ID: V-97737
Legacy ID: SV-106841

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 an ACF command screen enter:
SET CONTROL(GSO)
LIST PSWD

If "MINPSWD" is set to "8", this is not a finding.

Fix Text: Configure the Password option "MINPSWD" to "8".

CCI: CCI-000205

Group ID (Vulid): V-223517
Group Title: SRG-OS-000032-GPOS-00013
Rule ID: SV-223517r861171_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-FT-000010
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-97739
Legacy ID: SV-106843

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.

SMF data collection is the basic unit of tracking of all system functions and actions. Included in this tracking data are the audit records from each of the ACPs and system. If the required SMF data record types are not being collected, then accountability cannot be monitored, and its use in the execution of a contingency plan could be compromised.

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 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.

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.

Satisfies: SRG-OS-000032-GPOS-00013, SRG-OS-000392-GPOS-00172

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

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-223518
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223518r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-FT-000020
Rule Title: IBM z/OS data sets for the FTP Server must be properly protected.
Legacy ID: V-97741
Legacy ID: SV-106845

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 FTP server Started task (usually FTPD). Refer to the data set defined on the SYSFTPD DD statement.

If the 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.

Refer to the BANNER statement in the FTP Data configuration file. If the BANNER statement refers to an MVS data set and WRITE and ALLOCATE access to the data set containing the FTP banner file is restricted to systems programming personnel, this is not a finding.

If READ access to the data set containing the FTP banner file is permitted to all authenticated users, this is not a finding.

NOTES: The MVS data sets mentioned above are not used in every configuration. Absence of a data set will not be considered a finding.

Fix Text: Review the data set access authorizations defined to the ESM for the FTP.DATA and FTP.BANNER files. Configure these data sets to be protected as follows:

The data set containing the FTP.DATA configuration file allows read access to all authenticated users and all other access is restricted to systems programming personnel.

All write and allocate access to the data set containing the FTP.DATA configuration file is

logged.

The data set containing the FTP banner file allows read access to all authenticated users and all other access is restricted to systems programming personnel.

CCI: CCI-000213

Group ID (Vulid): V-223519
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223519r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-FT-000030
Rule Title: IBM z/OS permission bits and user audit bits for HFS objects that are part of the FTP Server component must be properly configured.
Legacy ID: V-97743
Legacy ID: SV-106847

Vulnerability Discussion: MVS data sets of the FTP Server provide the configuration and operational characteristics of this product. Failure to properly secure these data sets may lead to unauthorized access resulting in the compromise of the integrity and availability of customer data and some system services.

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: Ensure the UNIX permission bits and user audit bits on the HFS directories and files for the FTP Server 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-223520
Group Title: SRG-OS-000023-GPOS-00006
Rule ID: SV-223520r864503_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-FT-000040
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: V-97745
Legacy ID: SV-106849

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.

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 as specified below 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-223522
Group Title: SRG-OS-000228-GPOS-00088
Rule ID: SV-223522r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-FT-000060
Rule Title: IBM z/OS FTP.DATA configuration statements for the FTP Server must specify the BANNER statement.
Legacy ID: SV-106853
Legacy ID: V-97749

Vulnerability Discussion: The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Check Content:
Refer to the Data configuration file specified on the SYSFTPD DD statement in the FTP started task JCL.

If the BANNER statement is coded, this is not a finding.

Fix Text: Configure the FTP.DATA CONFIGURATION STATEMENT to include the following:

BANNER [An HFS file, e.g., /etc/ftp.banner]

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

Group ID (Vulid): V-223523
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223523r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-FT-000070
Rule Title: IBM z/OS FTP Control cards must be properly stored in a secure PDS file.
Legacy ID: SV-106855
Legacy ID: V-97751

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:
Provide a 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. The list must indicate which application uses the PDS, and access requirements for those PDSes (who and what level of access). Lists/spreadsheet used for documenting the meeting of this requirement must be maintained by the responsible Application/AIS Team, available upon request and not maintained by Mainframe ISSO.

Obtain the list/spreadsheet from the Application/AIS Team.

Access to FTP scripts and/or data files located on host system(s) that contain FTP userid and or password will be restricted to those individuals responsible for the application connectivity and who have a legitimate requirement to know the userid and password on a remote system.

FTP Control Cards within In-stream JCL, within JCL libraries or open access libraries/data sets is a finding.

If there is anyone not listed within the spreadsheet by userid that has access of Read or greater to the FTP control cards, this is a finding.

Fix Text: Create a list or spreadsheet of the locations where FTP control cards are stored, who should have access to those libraries, and which applications the FTP control cards are for.

Add Columns for all people permitted access to the secured PDS.

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-000366

Group ID (Vulid): V-223524
Group Title: SRG-OS-000368-GPOS-00154
Rule ID: SV-223524r853535_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-FT-000080
Rule Title: The IBM z/OS TFTP Server program must be properly protected.
Legacy ID: SV-106857
Legacy ID: V-97753

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 ACF Command screen enter:
SET CONTROL(GSO)
LIST LIKE(PPGM-)

If Programs TFTPD and EZATD are not defined in the GSO PPGM record, this is a finding.

From the ACF Command screen enter:
SET RESOURCE(PGM)
LIST LIKE(-)

If Program resources TFTPD and EZATD are not defined in the PROGRAM resource class, this is a finding.

If No access to the program resources TFTPD and EZATD is permitted, this is not a finding.

Fix Text: Configure the resource controls for the TFTP Server programs TFTPD and EZATD and ensure all access is restricted.

Evaluate the impact of implementing the following change. Develop a plan of action and implement the change as required.

Configure the resource controls for the TFTP Server programs TFTPD and EZATD and ensure all access is restricted.

Examples:
SET CONTROL(GSO)
CHANGE PPGM PGM-MASK(TFTPD EZATD) ADD

F ACF2,REFRESH(PPGM)

$KEY(TFTPD) TYPE(PGM)
UID(*) PREVENT

SET R(PGM)
COMPILE 'ACF2.MVA.PGM(TFTPD)' STORE

F ACF2,REBUILD(PGM)

$KEY(EZATD) TYPE(PGM)
UID(*) PREVENT

SET R(PGM)
COMPILE 'ACF2.MVA.PGM(EZATD)' STORE

F ACF2,REBUILD(PGM)

CCI: CCI-001764

Group ID (Vulid): V-223525
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223525r861172_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-FT-000090
Rule Title: IBM z/OS FTP Server daemon must be defined with proper security parameters.
Legacy ID: SV-106859
Legacy ID: V-97755

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 enter:
ACF
SET LID
LIST LIKE(FTP-) SECTION(ALL) PROFILE(OMVS)
NOTE: The JCL member is typically named FTPD.

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

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

The FTP daemon logonid is FTPD.
The FTPD logonid is defined with the STC attribute.

The FTPD logonid has the following z/OS UNIX attributes: UID(0), HOME directory '/', shell program /bin/sh.

Fix Text: Define the FTP daemon to run under its own user account. Specifically, it does not share the account defined for the z/OS UNIX kernel.

Define the FTP Server daemon account, privileges, and access authorizations to the ACP using the requirements below.

The following commands can be used to create the user account that is required for the FTP daemon:

SET LID
INSERT FTPD NAME(FTPD) GROUP(STCTCPX) STC

SET PROFILE(USER) DIVISION(OMVS)
INSERT FTPD UID(0) HOME(/) PROGRAM(/bin/sh)

F ACF2,REBUILD(USR),CLASS(P)

CCI: CCI-000764

Group ID (Vulid): V-223526
Group Title: SRG-OS-000163-GPOS-00072
Rule ID: SV-223526r861173_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-FT-000100
Rule Title: IBM z/OS startup parameters for the FTP Server must be defined in the SYSTCPD and SYSFTPD DD statements for configuration files.
Legacy ID: SV-106861
Legacy ID: V-97757

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-223527
Group Title: SRG-OS-000163-GPOS-00072
Rule ID: SV-223527r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-FT-000110
Rule Title: IBM z/OS FTP.DATA configuration for the FTP Server must have INACTIVE statement properly set.
Legacy ID: V-97759
Legacy ID: SV-106863

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 Data configuration file specified on the SYSFTPD DD statement in the FTP started task JCL.

If the INACTIVE statement is coded with a value between 1 and 900 (seconds) this is not a finding.

Fix Text: Configure the FTP.DATA CONFIGURATION STATEMENT to include the following:

INACTIVE [A value between 1 and 900]

CCI: CCI-001133

Group ID (Vulid): V-255895
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-255895r877345_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-FT-000120
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-255932
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-255932r881288_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-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-255933
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-255933r881291_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-IC-000020
Rule Title: IBM Integrated Crypto Service Facility (ICSF) install data sets must be properly protected.
Legacy ID: V-16932
Legacy ID: SV-30547

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:

If the ESM dataset rules for the IBM Integrated Crypto Service Facility (ICSF) install data sets does not restrict UPDATE and/or ALTER access to systems programming personnel this is a finding.

If the ESM data set rules for IBM Integrated Crypto Service Facility (ICSF) install data set does not specify that all (i.e., failures and successes) UPDATE and/or ALTER 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:

$KEY(SYS1)
CSF.- UID(syspaudt) R(A) W(L) A(L) E(A)
CSF.- UID(tstcaudt) R(A) W(L) A(L) E(A)
CSF.- UID(icsfusrs) R(A) E(A)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-255945
Group Title: SRG-OS-000259-GPOS-00100
Rule ID: SV-255945r881328_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-IC-000030
Rule Title: IBM Integrated Crypto Service Facility (ICSF) STC data sets must be properly protected.
Legacy ID: SV-30551
Legacy ID: V-17067

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 ACF2 data set access authorizations does not restrict READ access to auditors this is a finding

If the ACF2 data set access authorizations does not restrict WRITE and/or greater access to systems programming personnel this is a finding.

If the ACF2 data set access authorizations does not restrict WRITE and/or greater access to the product STC(s) and/or batch job(s) this is a finding.

Fix Text: Ensure that WRITE and/or greater access to IBM Integrated Crypto Service Facility (ICSF) STC data sets are limited to system programmers and ICSF STC and/or batch jobs only. READ access can be given to auditors at the ISSOs 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:

$KEY(SYS3)
CSF.- UID(syspaudt) R(A) W(A) A(A) E(A)
CSF.- UID(tstcaudt) R(A) W(A) A(A) E(A)
CSF.- UID(icsfstc) R(A) W(A) A(A) E(A)

CSF.- UID(audtaudt) R(A) E(A)

CCI: CCI-001499

Group ID (Vulid): V-255934
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-255934r881294_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-IC-000040
Rule Title: IBM Integrated Crypto Service Facility (ICSF) Started Task name must be properly identified / defined to the system ACP.
Legacy ID: SV-30578
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:
From the ACF command screen enter:
SET LID
SET VERBOSE
LIST IF(MUSASS)
LIST IF(STC)

If the logonid for the IBM Integrated Crypto Service Facility (ICSF) started task does not include MUSASS and/or NO-SMC, this is a finding.

Fix Text: 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:

INSERT CSFSTART NAME(STC, ICSF) NO-SMC STC

CCI: CCI-000764

Group ID (Vulid): V-223528
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223528r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-JS-000010
Rule Title: IBM z/OS JESTRACE and/or SYSLOG resources must be protected in accordance with security requirements.
Legacy ID: V-97761
Legacy ID: SV-106865

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 ACF command screen enter:
Set RESOURCE(SPL)
List like(localnodeid-)

If the following resources in the JESSPOOL resource class (i.e., TYPE(SPL)) are configured as noted below, this is not a finding.

localnodeid.JES2.$TRCLOG.taskid.-.JESTRACE
localnodeid.+MASTER+.SYSLOG.jobid.-.SYSLOG or
localnodeid.+BYPASS+.SYSLOG.jobid.-.SYSLOG

NOTE: These resource rules 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: 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 access authorization for the resources mentioned above is restricted to the following, this is not a finding.

Logonid(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: NOTE: If CLASMAP defines JESSPOOL as anything other than TYPE(SPL), replace SPL below with the appropriate three letters.

Configure the following resources in the JESSPOOL resource class (i.e., TYPE(SPL)):

localnodeid.JES2.$TRCLOG.taskid.-.JESTRACE
localnodeid.+MASTER+.SYSLOG.jobid.-.SYSLOG or
localnodeid.+BYPASS+.SYSLOG.jobid.-.SYSLOG

NOTE: These resource rules may be more generic as long as they pertain directly to the JESTRACE and SYSLOG data sets. For example:
localnodeid.JES2.-.-.-.JESTRACE
localnodeid.+MASTER+.-.-.-.- or
localnodeid.+BYPASS+.-.-.-.-

NOTE: 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.

Configure access authorization for the resources mentioned above is restricted to the following:

Logonid(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.

Example:
SET R(SPL)
$KEY(localnodeid) TYPE(SPL)
-.SYSLOG.-.-.- UID(sysprgmr) ALLOW
-.SYSLOG.-.-.- UID(seca) ALLOW
-.SYSLOG.-.-.- UID(appdudt) SERVICE(READ) ALLOW
-.SYSLOG.-.-.- UID(apps) SERVICE(READ) ALLOW
-.$TRCLOG.-.-.- UID(sysprgmr) ALLOW
-.$TRCLOG.-.-.- UID(seca) ALLOW
- UID(*) PREVENT

CCI: CCI-000213

Group ID (Vulid): V-223529
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223529r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-JS-000020
Rule Title: IBM z/OS JESSPOOL resources must be protected in accordance with security requirements.
Legacy ID: V-97763
Legacy ID: SV-106867

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 ACF command screen enter:
SET CONTROL(GSO)
LIST LIKE(CLASMAP-) {to determine the resource class for JESSPOOL}

NOTE: If CLASMAP defines JESSPOOL as anything other than TYPE(SPL), replace SPL below with the appropriate three letters.

SET RESOURCE(SPL)
LIST LIKE(-)

If the following resources are defined to the JESSPOOL resource class (i.e., TYPE(SPL)) with a default access of PREVENT, this is not a finding.

localnodeid.-
localnodeid.JES2.$TRCLOG.taskid.-.JESTRACE
localnodeid.+MASTER+.SYSLOG.jobid.-.SYSLOG

These resource rules may be more generic as long as they pertain directly to the JESTRACE and SYSLOG data sets. For example:
localnodeid.JES2.-.-.-.JESTRACE
localnodeid.+MASTER+.-.-.-.-

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.

If the following resource is defined to the JESSPOOL resource class (i.e., TYPE(SPL)) with a default access of READ, this is not a finding.
localnodeid.jesid.$JESNEWS.taskid.Dnewslvl.JESNEWS
jesid The logonid associated with your JES2 system.

NOTE: This resource rule may be more generic as long as it pertains directly to the JESNEWS data set. For example:
localnodeid.jesid.$JESNEWS.-.-.JESNEWS

Fix Text: NOTE: If CLASMAP defines JESSPOOL as anything other than TYPE(SPL), replace SPL below with the appropriate three letters.

Configure the CLASMAP record to define the JESSPOOL resource class.

Example:
SHOW CLASMAP

The following resources are defined to the JESSPOOL resource class (i.e., TYPE(SPL)) with a default access of PREVENT:
localnodeid.-
localnodeid.JES2.$TRCLOG.taskid.-.JESTRACE
localnodeid.+MASTER+.SYSLOG.jobid.-.SYSLOG

Example:
$KEY(localnodeid) TYPE(SPL)
- UID(*) PREVENT

These resource rules may be more generic as long as they pertain directly to the JESTRACE and SYSLOG data sets. For example:
localnodeid.JES2.-.-.-.JESTRACE
localnodeid.+MASTER+.-.-.-.-

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 resource is defined to the JESSPOOL resource class (i.e., TYPE(SPL)) with a default access of READ:
localnodeid.jesid.$JESNEWS.taskid.Dnewslvl.JESNEWS

jesid The logonid associated with your JES2 system.

This resource rule may be more generic as long as it pertains directly to the JESNEWS data set. For example:
localnodeid.jesid.$JESNEWS.-.-.JESNEWS

CCI: CCI-000213

Group ID (Vulid): V-223530

Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223530r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-JS-000030
Rule Title: IBM z/OS JESNEWS resources must be protected in accordance with security requirements.
Legacy ID: V-97765
Legacy ID: SV-106869

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 ACF command screen enter:
SET RESOURCE(OPR)
LIST LIKE(JES-)

If the JES2.UPDATE.JESNEWS resource is defined to the OPERCMDS resource class with a default access of PREVENT, this is not a finding.

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 DELETE service 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 the resource rules for the OPERCMDS resource class (i.e., TYPE(OPR)) and ensure the following items are in effect:

1) The JES2.UPDATE.JESNEWS resource is defined to the OPERCMDS resource class with a default access of PREVENT.

2) Access authorization to the JES2.UPDATE.JESNEWS resource in the OPERCMDS class restricts DELETE service to the appropriate personnel (i.e., users responsible for maintaining the JES News data set) and all access is logged.

Example:
$KEY(JES2) TYPE(OPR)
UPDATE.JESNEWS UID(SYSPROG) SERVICE(READ,UPDATE) LOG
UPDATE.JESNEWS UID(*) PREVENT

CCI: CCI-000213

Group ID (Vulid): V-223531
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223531r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-JS-000040
Rule Title: IBM z/OS JES2 system commands must be protected in accordance with security requirements.
Legacy ID: V-97767
Legacy ID: SV-106871

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:
NOTE: If CLASMAP defines OPERCMDS as anything other than TYPE(OPR), replace OPR

below with the appropriate three letters.

From the ACF command screen enter:
SET RESOURCE(OPR)
LIST LIKE(JES-)

If the JES2.- resource is defined to the OPERCMDS class with a default access of PREVENT and all access is logged, this is not a finding.

If access to JES2 system commands defined in the table in the IBM JES2 Initialization and Tuning Guide titled "JES2 commands with profile names and minimum required authority" is restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users), this is not a finding.

If all elevated access to JES2 system commands is logged, this is not a finding.

Fix Text: Review the GSO definitions. If CLASMAP defines OPERCMDS as anything other than TYPE(OPR), replace OPR below with the appropriate three letters.

Review resource rules for TYPE(OPR).

Define the JES2.- resource is defined to the OPERCMDS class with a default access of PREVENT and all access is logged.

Define access to JES2 system commands defined in the JES2 system commands defined in the table in the IBM JES2 Initialization and Tuning Guide entitled 'JES2 commands with profile names and minimum required authority' is restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users).

Define access to specific JES2 system commands is logged as indicated in the table JES2 system commands defined in the table in the IBM JES2 Initialization and Tuning Guide titled "JES2 commands with profile names and minimum required authority".

Assure that elevated access is logged.

Some ACF2 Examples:
$KEY(JES2) TYPE(OPR)
CANCEL.BAT UID(oper) SERVICE(READ,UPDATE) LOG
DISPLAY.JOB UID(*) SERVICE(READ) LOG
START.INITIATOR UID(oper) SERVICE(DELETE) LOG
START.LINE UID(oper) SERVICE(DELETE) LOG
STOP.INITIATOR UID(oper) SERVICE(DELETE) LOG
STOP.LINE UID(oper) SERVICE(DELETE) LOG
- UID(*) PREVENT

CCI: CCI-000213

Group ID (Vulid): V-223532
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223532r861174_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-JS-000050
Rule Title: IBM z/OS JES2 spool resources must be controlled in accordance with security requirements.
Legacy ID: SV-106873
Legacy ID: V-97769

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 there ACF Command screen enter:
SET RESOURCE(SPL)
LIST LIKE(localnodeid-)

If the accesses to the JESSPOOL resources are properly restricted using the following guidance, this is not a finding.

NOTE: If CLASMAP defines JESSPOOL as anything other than TYPE(SPL), replace SPL below with the appropriate three letters.

Review the JESSPOOL report for resource rules with the following naming convention. These rules may be fully qualified, be specified as generic, or be specified with masking as indicated below:

localnodeid.logonid.jobname.jobid.dsnumber.name

localnodeid - The name of the node on which the SYSIN or SYSOUT data set currently resides.
logonid - The logonid associated with the job. This is the logonid ACF2 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 have access to their own JESSPOOL resources.

The localnodeid. resource will be restricted to only system programmers, operators, and automated operations personnel, with access to allow all SERVICEs or any combination of SERVICE(...). 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, SERVICE(READ, UPDATE, DELETE, ADD). 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 JESSPOOL resources as defined below.

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 (?).

The CLASMAP defines JESSPOOL as TYPE(SPL).

Example:
SHOW CLASMAP

By default a user has access only to that user's own JESSPOOL resources. However, situations exist where a user legitimately requires access to jobs that run under another user's userid. In particular, if a user routes SYSOUT to an external writer, the external writer should have access to that user's SYSOUT.

The localnodeid. resource will be restricted to only system programmers, operators, and automated operations personnel with access to allow all SERVICEs or any combination of SERVICE(READ, UPDATE, DELETE, ADD). All access will be logged. (localnodeid. resource includes all generic and/or masked permissions, example: localnodeid.-.-, localnodeid.-, etc)

Example:
SET R(SPL)
$KEY(localnode) TYPE(SPL)
- UID(sysprgmr) SERVICE(UPDATE,READ) LOG
- UID(*) PREVENT

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, SERVICE(READ, UPDATE, DELETE, ADD). 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:
SET R(SPL)
$KEY(localnode) TYPE(SPL)
UMO- UID(UML03IGUSRZSS***UMO) SERVICE(UPDATE,READ) LOG
- UID(*) PREVENT

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 must be removed.

CCI: CCI-000213

Group ID (Vulid): V-223533
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223533r861175_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-JS-000060
Rule Title: IBM z/OS JES2 output devices must be properly controlled for Classified Systems.
Legacy ID: SV-106875
Legacy ID: V-97771

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.

Verify that the accesses for WRITER resources are restricted.

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

The ACF2 resources and/or generic equivalent are defined with a default access of PREVENT.

The ACF2 resources and/or generic equivalent identified below will be defined with access restricted to the operators and system programming personnel:

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

NOTE: Common sense should prevail during the analysis. For example, access to the offload output destinations should be limited to only systems personnel (e.g., operations staff/system programmers) on a classified system.

Fix Text: Configure the 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-223534

Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223534r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-JS-000070
Rule Title: IBM z/OS JES2 output devices must be controlled in accordance with the proper security requirements.
Legacy ID: SV-106877
Legacy ID: V-97773

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 ACF input screen enter:
SET CONTROL(GSO)
LIST LIKE(CLASMAP-) [To determine the resource class for WRITER]

NOTE: If CLASMAP defines WRITER as anything other than TYPE(WTR), replace WTR below with the appropriate three letters.

SET RESOURCE(WTR)
LIST LIKE(-)

If the JES2.- resource is defined to the WRITER resource class with a default access of PREVENT, this is not a finding.

If the other resources mentioned below are protected by generic and/or fully qualified rules defined to the WRITER resource class with a default access of PREVENT, this is not a finding.

If the ACF2 resources and/or generic equivalent identified below are defined with access restricted to the appropriate personnel, this is not a finding.

NOTE: A default access of READ is allowed for output destinations that are permitted to route output for all users. Currently, there is no guidance on which output destinations are appropriate for a default access of READ. However, common sense should prevail during the analysis. For example, a default access of READ would typically be inappropriate for RJE, NJE, and offload output destinations.

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.

OFFn, where n is the number of the offload transmitter. Determine the numbers by searching for OFF(in the JES2 parameters.

PRTn, where n is the number of the local printer. Determine the numbers by searching for PRT(in the JES2 parameters.

PUNn, where n is the number of the local card punch. Determine the numbers by searching for PUN(in the JES2 parameters.

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.

Rnnnn.PRm, where nnnn is the number of the remote workstation and m is the number of the printer. Determine the numbers by searching for .PR in the JES2 parameters.

Rnnnn.PUm, where nnnn is the number of the remote workstation and m is the number of the punch. Determine the numbers by searching for .PU in the JES2 parameters.

Fix Text: NOTE: If CLASMAP defines WRITER as anything other than TYPE(WTR), replace WTR below with the appropriate three letters.

Configure the WRITER resource class (i.e., TYPE(WTR)) as follows with:

JES2.- (backstop profile)
JES2.LOCAL.OFFn.- (spool offload transmitter)
JES2.LOCAL.OFFn.ST (spool offload SYSOUT transmitter)
JES2.LOCAL.OFFn.JT (spool offload job transmitter)
JES2.LOCAL.PRTn (local printer)
JES2.LOCAL.PUNn (local punch)
JES2.NJE.nodename (NJE node)
JES2.RJE.Rnnnn.PRm (remote printer)
JES2.RJE.Rnnnn.PUm (remote punch)

Ensure the following items are in effect:

The JES2.- resource is defined to the WRITER resource class with a default access of PREVENT.

The other resources mentioned above are protected by generic and/or fully qualified rules defined to the WRITER resource class with a default access of PREVENT.

NOTE: A default access of READ is allowed for output destinations that are permitted to route output for all users. Currently, there is no guidance on which output destinations are appropriate for a default access of READ. However, common sense should prevail during the analysis. For example, a default access of READ would typically be inappropriate for RJE, NJE, and offload output destinations.

Examples:
$KEY(JES2) TYPE(WTR)
LOCAL.OFF- UID(*) PREVENT
LOCAL.OFF-.JT UID(*) PREVENT
LOCAL.OFF-.ST UID(oper) SERVICE(READ) ALLOW
LOCAL.OFF-.ST UID(sysprgmr) SERVICE(READ) ALLOW
LOCAL.OFF-.ST UID(seca) SERVICE(READ) ALLOW
LOCAL.OFF-.ST UID(*) PREVENT
LOCAL.PRT- UID(*) SERVICE(READ) ALLOW
LOCAL.PUN- UID(*) PREVENT
NJE.- UID(*) SERVICE(READ) ALLOW
RJE.- UID(sysprgmr) SERVICE(READ) ALLOW
RJE.- UID(*) PREVENT
- UID(*) PREVENT

CCI: CCI-000213

Group ID (Vulid): V-223535
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223535r767056_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-JS-000080
Rule Title: IBM z/OS JES2 input sources must be controlled in accordance with the proper security requirements.
Legacy ID: SV-106879
Legacy ID: V-97775

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 ACF input screen enter:
SET CONTROL(GSO)
LIST LIKE(CLASMAP-)
Or
SHOW CLASMAP {to determine the resource type for JESINPUT}
NOTE: If CLASMAP defines JESINPUT as anything other than TYPE(INP), replace INP below with the appropriate three letters.

SET RESOURCE(INP)
LIST LIKE(-)

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.

Nodename is the NAME parameter in the NODE statement. Review the NJE node definitions by searching for NODE(in the JES2 parameters.

OFFn, where n is the number of the offload receiver. Review the spool offload receiver definitions by searching for OFF(in the JES2 parameters.

Rnnnn, where nnnn is the number of the remote workstation. Review the RJE node definitions by searching for RMT(in the JES2 parameters.

RDRnn, where nn is the number of the reader. Review the reader definitions by searching for RDR(in the JES2 parameters.

If the resources mentioned below are protected by generic and/or fully qualified rules defined to the JESINPUT resource class this is not a finding.

If a default access of PREVENT is specified for all resources this is not a finding.

If the ACF2 resources and/or generic equivalent identified below are defined with access

restricted to the appropriate personnel this is not a finding.

NOTE: Use common sense during the analysis. For example, access to the offload input sources should be limited to systems personnel (e.g., operations staff).

NOTE: A default access of READ is allowed for input sources that are permitted to submit jobs for all users. No guidance on which input sources are appropriate for a default access of READ. However, common sense should prevail during the analysis. For example, a default access of READ would typically be inappropriate for RJE, NJE, offload, and STC input sources.

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)

Fix Text: NOTE: If CLASMAP defines JESINPUT as anything other than TYPE(INP), replace INP below with the appropriate three letters.

Configure resources in the JESINPUT resource class (i.e., TYPE(INP)) granting read access to authorized users for each of the following input resources:
INTRDR (internal reader for batch jobs)
nodename (NJE node)
OFFn.- (spool offload receiver)
OFFn.JR (spool offload job receiver)
OFFn.SR (spool offload SYSOUT receiver)
Rnnnn.RDm (RJE workstation)
RDRnn (local card reader)
STCINRDR (internal reader for started tasks)
TSUINRDR (internal reader for TSO logons)

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.

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 JES2 parameters.

OFFn, where n is the number of the offload receiver. Determine the numbers by searching for OFF(in the JES2 parameters.

Rnnnn.RDm, where nnnn is the number of the remote workstation and m is the number of the

reader. Determine the numbers by searching for .RD in the JES2 parameters.

RDRnn, where nn is the number of the reader. Determine the numbers by searching for RDR(in the JES2 parameters.

Ensure the following items are in effect:

The CLASMAP record defines the JESINPUT resource class.

Example:
SHOW CLASMAP

The resources mentioned in (b) are protected by generic and/or fully qualified rules defined to the JESINPUT resource class.

A default access of PREVENT is specified for all resources.

NOTE: A default access of READ is allowed for input sources that are permitted to submit jobs for all users. Currently, there is no guidance on which input sources are appropriate for a default access of READ. However, common sense should prevail during the analysis. For example, a default access of READ would typically be inappropriate for RJE, NJE, offload, and STC input sources.

Examples:
$KEY(STCINRDR) TYPE(INP)
- UID(*) PREVENT

$KEY(TSUINRDR) TYPE(INP)
- UID(*) PREVENT

$KEY(RDR*****) TYPE(INP)
$MEMBER(RDR#####)
- UID(*) PREVENT

$KEY(OFF*****) TYPE(INP)
$MEMBER(OFF#####)
JR UID(oper) SERVICE(READ)
JR UID(*) PREVENT
SR UID(oper) SERVICE(READ)
SR UID(*) PREVENT
- UID(oper) SERVICE(READ)
- UID(*) PREVENT

CCI: CCI-000213

Group ID (Vulid): V-223536
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223536r853536_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-JS-000090
Rule Title: IBM z/OS Surrogate users must be controlled in accordance with proper security requirements.
Legacy ID: SV-106881
Legacy ID: V-97777

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:
Review the ACFGSO report executionuserid.SUBMIT resources. These are usually defined to CLASMAP as TYPE(SUR).
NOTE: If CLASMAP defines SURROGAT as anything other than TYPE(SUR), replace SUR below with the appropriate three letters.

If no executionuserid.SUBMIT resources are defined to the SURROGAT resource class, this is not applicable.

If executionuserid.SUBMIT resources are defined to the SURROGAT resource class, review resource rules for TYPE(SUR). If the following items are in effect, this is not a finding.

All executionlogonid.SUBMIT resources defined to the SURROGAT class specify a default access of PREVENT.

All resource access is logged; at the discretion of the ISSM/ISSO, scheduling tasks may be exempted.

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: All executionuserid.SUBMIT resources defined to the SURROGAT resource class specify a default of no access; all resource access is logged (at the discretion of the ISSM/ISSO scheduling tasks may be exempted) and access authorization is restricted to the minimum number of personnel required for running production jobs.

Ensure the CLASMAP defines SURROGAT as TYPE(SUR).

NOTE: If CLASMAP defines SURROGAT as anything other than TYPE(SUR), replace SUR below with the appropriate three letters.

Ensure the following items are in effect:

All executionlogonid.SUBMIT resources defined to the SURROGAT class specify a default access of PREVENT.

All resource access is logged except for scheduling tasks.

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 Executionuserid.SUBMIT resources:

Keep the use of Executionuserid.SUBMIT resources outside of those granted to the scheduling software to a minimum number of individuals.

The simplest configuration is to only use Executionuserid.SUBMIT 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, Executionuserid.SUBMIT usage should not become the default for all jobs submitted by individual userids (i.e., system programmer must use their assigned individual userids for software installation, duties, whereas using a Executionuserid.SUBMIT resource would normally be 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.

Example:

$KEY(SRR) TYPE(SUR)
SUBMIT UID(*******STC******CONTROLM) ALLOW
- UID(*) PREVENT

CCI: CCI-000213

CCI: CCI-002233

Group ID (Vulid): V-223537
Group Title: SRG-OS-000032-GPOS-00013
Rule ID: SV-223537r836653_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000010
Rule Title: The IBM z/OS BPX.SMF resource must be properly configured.
Legacy ID: V-97779
Legacy ID: SV-106883

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 cyber attacks 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 ACF2 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-223539
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-223539r836655_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000030
Rule Title: IBM z/OS Inapplicable PPT entries must be invalidated.
Legacy ID: V-97783
Legacy ID: SV-106887

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 non-existent 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-223540
Group Title: SRG-OS-000277-GPOS-00107
Rule ID: SV-223540r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000040
Rule Title: IBM z/OS system administrator must develop a process notify appropriate personnel when accounts are removed.
Legacy ID: V-97785
Legacy ID: SV-106889

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-223541
Group Title: SRG-OS-000275-GPOS-00105
Rule ID: SV-223541r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000050
Rule Title: IBM z/OS system administrator must develop a process notify appropriate personnel when accounts are modified.
Legacy ID: V-97787
Legacy ID: SV-106891

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 modify an existing account. Notification of account modification is one method for mitigating this risk. A comprehensive account management process will ensure an audit trail which documents the modification of operating system user accounts and notifies the system administrator and ISSO of changes. 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-223542
Group Title: SRG-OS-000276-GPOS-00106
Rule ID: SV-223542r533198_rule
Severity: CAT II

Rule Version (STIG-ID): ACF2-OS-000060
Rule Title: IBM z/OS system administrator must develop a process notify appropriate personnel when accounts are deleted.
Legacy ID: SV-106893
Legacy ID: V-97789

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:
Develop a documented develop a 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-223543
Group Title: SRG-OS-000274-GPOS-00104
Rule ID: SV-223543r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000070
Rule Title: IBM z/OS system administrator must develop a process notify appropriate personnel when accounts are created.
Legacy ID: SV-106895
Legacy ID: V-97791

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-223544
Group Title: SRG-OS-000004-GPOS-00004
Rule ID: SV-223544r869034_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000080
Rule Title: IBM z/OS Required SMF data record types must be collected.
Legacy ID: SV-106897
Legacy ID: V-97793

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.

SMF data collection is the basic unit of tracking of all system functions and actions. Included in this tracking data are the audit records from each of the ACPs and system. If the required SMF data record types are not being collected, then accountability cannot be monitored, and its use in

the execution of a contingency plan could be compromised.

Satisfies: SRG-OS-000004-GPOS-00004, 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-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000255-GPOS-00096, SRG-OS-000303-GPOS-00120, SRG-OS-000327-GPOS-00127, SRG-OS-000365-GPOS-00152, SRG-OS-000392-GPOS-00172, 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-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

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-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-002130

CCI: CCI-002234

CCI: CCI-002884

Group ID (Vulid): V-223545
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223545r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000090
Rule Title: IBM z/OS special privileges must be assigned on an as-needed basis to LOGONIDs associated with STCs and LOGONIDs that need to execute TSO in batch.
Legacy ID: SV-106899
Legacy ID: V-97795

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:
ACF
SET LID
SET VERBOSE
LIST IF(ACCTPRIV OR CONSOLE OR OPERATOR OR MOUNT)

If the ACCTPRIV privilege is restricted to security personnel, this is not a finding.

If the CONSOLE and OPERATOR privileges are restricted to authorized systems personnel (e.g., systems programming personnel, operations staff, etc), this is not a finding.

If the MOUNT privilege is restricted to DASD batch users only, this is not a finding.

Fix Text: Review all Logonids for the following and ensure that only authorized users with justification are given access to the privileges.

The ACCTPRIV privilege is restricted for used to the domain level security personnel (ISSO/ISSM).

The CONSOLE and OPERATOR privileges are restricted to authorized systems personnel (e.g., systems programming personnel, operations staff, etc).

The MOUNT privilege is restricted to DASD batch users only on an as-needed basis to execute TSO in batch.

Ensure that all privileges are kept to a minimum and are controlled and documented.

CCI: CCI-000213

Group ID (Vulid): V-223546
Group Title: SRG-OS-000038-GPOS-00016

Rule ID: SV-223546r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000100
Rule Title: IBM z/OS must specify SMF data options to assure appropriate activation.
Legacy ID: SV-106901
Legacy ID: V-97797

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.

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-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

Check Content:
Refer to IEASYS00 member in SYS1.PARMLIB Concatenation. Determine proper SMFPRMxx member.

If the following SMF collection options are specified as stated below, this is not a finding.

The settings for several parameters are critical to the collection process:

ACTIVE - Activates the collection of SMF data.

MAXDORM - 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 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 listed.

CCI: CCI-000131

CCI: CCI-000132

CCI: CCI-000133

CCI: CCI-000134

CCI: CCI-000135

CCI: CCI-001464

CCI: CCI-001665

Group ID (Vulid): V-223547
Group Title: SRG-OS-000341-GPOS-00132
Rule ID: SV-223547r877391_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000110
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-106903
Legacy ID: V-97799

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 the system.

If the output data sets in the procedure have storage capacity to store at least one week's worth of audit data, this is not a finding.

Fix Text: Make sure output file and dump procedures allow storage capacity to store one week's worth of audit data.

CCI: CCI-001849

Group ID (Vulid): V-223548
Group Title: SRG-OS-000342-GPOS-00133

Rule ID: SV-223548r877390_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000120
Rule Title: IBM z/OS system administrators must develop an automated process to collect and retain SMF data.
Legacy ID: V-97801
Legacy ID: SV-106905

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: The ISSO will ensure that an automated process is in place to collect SMF data.

Review SMF data collection and retention processes. Verify processes 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, the site will 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, or
- Establish a process using Audit logging.

CCI: CCI-001851

Group ID (Vulid): V-223549
Group Title: SRG-OS-000046-GPOS-00022
Rule ID: SV-223549r853542_rule

Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000130
Rule Title: IBM z/OS BUFUSEWARN in the SMFPRMxx must be properly set.
Legacy ID: V-97803
Legacy ID: SV-106907

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.

Satisfies: SRG-OS-000046-GPOS-00022, SRG-OS-000343-GPOS-00134, SRG-OS-000344-GPOS-00135

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

CCI: CCI-001855

CCI: CCI-001858

Group ID (Vulid): V-223550
Group Title: SRG-OS-000047-GPOS-00023
Rule ID: SV-223550r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000140

Rule Title: IBM z/OS NOBUFFS in SMFPRMxx must be properly set (Default is MSG).
Legacy ID: V-97805
Legacy ID: SV-106909

Vulnerability Discussion: It is critical that when the operating system is at risk of failing to process audit logs as required, it takes action to mitigate the failure. Audit processing failures include: software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded. Responses to audit failure depend upon the nature of the failure mode.

When availability is an overriding concern, other approved actions in response to an audit failure are as follows:

1) If the failure was caused by the lack of audit record storage capacity, the operating system must continue generating audit records if possible (automatically restarting the audit service if necessary), overwriting the oldest audit records in a first-in-first-out manner.

2) If audit records are sent to a centralized collection server and communication with this server is lost or the server fails, the operating system must queue audit records locally until communication is restored or until the audit records are retrieved manually. Upon restoration of the connection to the centralized collection server, action should be taken to synchronize the local audit data with the collection server.

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-223551
Group Title: SRG-OS-000355-GPOS-00143
Rule ID: SV-223551r877038_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000150
Rule Title: IBM z/OS SNTP daemon (SNTPD) permission bits must be properly configured.

Legacy ID: V-97807
Legacy ID: SV-106911

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-223552
Group Title: SRG-OS-000355-GPOS-00143
Rule ID: SV-223552r877038_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000160
Rule Title: IBM z/OS SNTP daemon (SNTPD) must be active.
Legacy ID: V-97809
Legacy ID: SV-106913

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:
Verify the operating system, for networked systems, compares internal information system clocks at least every 24 hours with a server which is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, or a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).

If it does not, 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-223553
Group Title: SRG-OS-000356-GPOS-00144
Rule ID: SV-223553r853545_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000170
Rule Title: IBM z/OS PARMLIB CLOCKxx must have the Accuracy PARM coded properly.
Legacy ID: V-97811
Legacy ID: SV-106915

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:
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-223554
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-223554r919119_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000180
Rule Title: IBM z/OS SMF collection files (i.e., SYS1.MANx) access must be limited to appropriate users and/or batch jobs that perform SMF dump processing.
Legacy ID: V-97813
Legacy ID: SV-106917

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, ACF2, 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 ACF2 data set rules for the SMF data collection files (e.g., SYS1.MAN* or IFASMF.SYS1.*) restrict ALLOCATE access to only z/OS systems programming personnel.
- The ACF2 data set rules for the SMF data collection files (e.g., SYS1.MAN* or IFASMF.SYS1.*) restrict WRITE access to z/OS systems programming personnel and/or batch

jobs that perform SMF dump processing and others as approved by the ISSM.
- The ACF2 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 ACF2 data set rules for SMF data collection files (e.g., SYS1.MAN* or IFASMF.SYS1.*) specify that all (i.e., failures and successes) WRITE and/or ALLOCATE access is logged.

Fix Text: Ensure that WRITE or greater 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.

READ 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 and/or ALLOCATE access are logged.

Ensure read access failures are logged.

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-000213

CCI: CCI-001314

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

CCI: CCI-002235

Group ID (Vulid): V-223556
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223556r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000200
Rule Title: IBM z/OS PASSWORD data set and OS passwords must not be used.
Legacy ID: SV-106921
Legacy ID: V-97817

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-223557
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223557r836661_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000210
Rule Title: IBM z/OS must configure system waittimes to protect resource availability based on site priorities.
Legacy ID: V-97819
Legacy ID: SV-106923

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:
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 ISSA 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-223558
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223558r803626_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000220
Rule Title: IBM z/OS Emergency LOGONIDs must be properly defined.
Legacy ID: V-97821
Legacy ID: SV-106925

Vulnerability Discussion: Activity under unusual conditions can indicate hostile activity. For example, what is normal activity during business hours can indicate hostile activity if it occurs during off hours.

Depending on mission needs and conditions, account usage restrictions based on conditions and circumstances may be critical to limit access to resources and data to comply with operational or mission access control requirements. Thus, the operating system must be configured to enforce the specific conditions or circumstances under which organization-defined accounts can be used (e.g., by restricting usage to certain days of the week, time of day, or specific durations of time).

Check Content:
Ask the system administrator to provide a list of all emergency logonids available to the site along with the associated function of each.
If there are no emergency logonids defined, ask the system administrator for an alternate documented procedure to handle emergencies. If there are no emergency logonids and no documented emergency procedure, this is a finding.

If emergency logonids exist, at a minimum, a logonid will exist with the security administration attributes specified in accordance with the following requirements:

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

ACCOUNT

JCL
JOB
MONITOR
NONON CNCL
RULEVLD

RSRCVLD
SECURITY
TSO
TSOPROC(xxxxxxxx)
TSOACCT(none)

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

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

JCL
JOB
MONITOR
NON CNCL (Will force logging of all activity.)
TSO
TSOPROC(xxxxxxxx)
TSOACCT(none)

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

All emergency logonid/logonid(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 logonid/logonid(s) will have distinct, different passwords in SYS1.UADS and in the ESM, 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 ESM.

All emergency logonid/logonid(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 logonid is released for use, its password is to be reset by the ISSO within 12 hours.

If all the emergency logonid items above are true, this is not a finding.

If any item above is untrue, this is a finding.

Fix Text: Ensure that Emergency Logonids use these fields to enforce restrictions for Emergency logonids.

Two classes of emergency logonids may exist. The following privileges and specifications will be used for these logonids:

Note: Only the emergency logonid with the security administration logonid attributes is required.

(1) For emergency IDs with the ability to access and update all system data sets, but which do not have security administration privileges:

NOFSRETAIN
JCL
JOB
MONITOR
NON CNCL (Will force logging of all activity.)
TSO
TSOPROC(xxxxxxxx)
TSOACCT(none)

Example:

SET LID
INSERT logonid NOFSRETAIN JCL JOB MONITOR NON-CNCL TSO TSOPRC(xxxxxxxx) TSOACCT(none)

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

ACCOUNT
NOFSRETAIN
JCL
JOB
MONITOR
NONON CNCL
RULEVLD
RSRCVLD
SECURITY
TSO
TSOPROC(xxxxxxxx)
TSOACCT(none)

Example:

SET LID
INSERT logonid ACCOUNT NOFSRETAIN JCL JOB MONITOR RULEVLD RSRCVLD NONON-CNCL SECURITY TSO TSOPRC(xxxxxxxx) TSOACCT(none)

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

CCI: CCI-000366

Group ID (Vulid): V-223559
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223559r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000230
Rule Title: IBM z/OS DFSMS control data sets must reside on separate storage volumes.
Legacy ID: V-97823
Legacy ID: SV-106927

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:
Review the logical parmlib data sets, example: SYS1.PARMLIB(IGDSMSxx), to identify the fully qualified file names for the following SMS data sets:
Active Control Data Set (ACDS)
Communications Data Set (COMMDS)

If the COMMDS and ACDS SMS data sets identified above reside on different volumes, this is not a finding.

If the COMMDS and ACDS SMS data sets identified above are collocated on the same volume, this is a finding.

Fix Text: Allocate the primary and backup SMS Control data sets on separate volumes.

Source Control Data Set (SCDS) contains a SMS configuration, which defines a storage management policy.

Active Control Data Set (ACDS) contains a copy of the most recently activated configuration. All systems in a SMS complex use this configuration to manage storage.

Communications Data Set (COMMDS) contains the name of the ACDS containing the currently active storage management policy, the current utilization statistics for each system managed volume, and other system information.

The ACDS data set will reside on a different volume than the COMMDS data set.

Allocate backup copies of the ADCS and COMMDS data sets on a different shared volume from the primary ACDS and COMMDS data sets.

CCI: CCI-000366

CCI: CCI-000549

Group ID (Vulid): V-223560
Group Title: SRG-OS-000480-GPOS-00232
Rule ID: SV-223560r853547_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000240
Rule Title: IBM z/OS Policy Agent must employ a deny-all, allow-by-exception firewall policy for allowing connections to other systems.
Legacy ID: V-97825
Legacy ID: SV-106929

Vulnerability Discussion: Failure to restrict network connectivity only to authorized systems permits inbound connections from malicious systems. It also permits outbound connections that may facilitate exfiltration of DoD data.

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-223561
Group Title: SRG-OS-000368-GPOS-00154
Rule ID: SV-223561r861180_rule

Severity: CAT I
Rule Version (STIG-ID): ACF2-OS-000250
Rule Title: Unsupported IBM z/OS system software must not be installed and/or active on the system.
Legacy ID: V-97827
Legacy ID: SV-106931

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.
- Require 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.
- Require 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 which is NO longer supported is a CAT I vulnerability. The customer and site will be given six months to mitigate the risk, come up with a supported solution, or obtain a formal letter approving such risk/software.

CCI: CCI-001764

Group ID (Vulid): V-223562
Group Title: SRG-OS-000368-GPOS-00154
Rule ID: SV-223562r853549_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000260
Rule Title: IBM z/OS must not allow non-existent or inaccessible LINKLIST libraries.
Legacy ID: V-97829
Legacy ID: SV-106933

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 LINKLINK 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:

-Avoid 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 non-existent libraries. The ISSO should modify and/or delete the rules associated with these libraries.

CCI: CCI-001764

Group ID (Vulid): V-223563
Group Title: SRG-OS-000368-GPOS-00154
Rule ID: SV-223563r853550_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000270
Rule Title: IBM z/OS must not allow non-existent or inaccessible Link Pack Area (LPA) libraries.
Legacy ID: SV-106935
Legacy ID: V-97831

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 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 should 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-223564
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-223564r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000280
Rule Title: IBM z/OS must not have inaccessible APF libraries defined.
Legacy ID: SV-106937
Legacy ID: V-97833

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-223565
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-223565r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000290
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-106939
Legacy ID: V-97835

Vulnerability Discussion: Failure to specify LINKAUTH=APFTAB allows libraries other than those designated as APF to contain authorized modules which could bypass security and violate the integrity of the operating system environment. This expanded authorization list inhibits the ability to control inclusion of these modules.

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-223566
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-223566r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000310
Rule Title: Duplicated IBM z/OS sensitive utilities and/or programs must not exist in APF libraries.
Legacy ID: SV-106941
Legacy ID: V-97837

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.

The organization must perform a periodic scan/review of the application (as required by CCI-

000384) and disable functions, ports, protocols, and services deemed to be unneeded or non-secure.

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 not you may receive insufficient access errors)

If any of the list of Sensitive Utilities exist in the duplicate APF modules return, 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-223567
Group Title: SRG-OS-000096-GPOS-00050
Rule ID: SV-223567r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000320
Rule Title: IBM z/OS must properly configure CONSOLxx members.
Legacy ID: SV-106943

Legacy ID: V-97839

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.

MCS consoles can be used to issue operator commands. Failure to properly control access to MCS consoles could result in unauthorized personnel issuing sensitive operator commands. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

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.

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-223568
Group Title: SRG-OS-000067-GPOS-00035
Rule ID: SV-223568r811030_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000330
Rule Title: IBM z/OS must use ICSF or SAF Key Rings for key management.
Legacy ID: V-97841
Legacy ID: SV-106945

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.

Satisfies: SRG-OS-000067-GPOS-00035, SRG-OS-000068-GPOS-00036

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 found, this is a finding.

Fix Text: Define all Keys/Certificates to ICSF or the security database. Remove any .kdb and .jks files.

CCI: CCI-000186

CCI: CCI-000187

Group ID (Vulid): V-223569
Group Title: SRG-OS-000185-GPOS-00079
Rule ID: SV-223569r853551_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000340
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-97843
Legacy ID: SV-106947

Vulnerability Discussion: Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive and tape drive, when used for backups) within an operating system.

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 they 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-001199

CCI: CCI-002450

CCI: CCI-002475

CCI: CCI-002476

Group ID (Vulid): V-223570
Group Title: SRG-OS-000138-GPOS-00069
Rule ID: SV-223570r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000350
Rule Title: IBM z/OS sensitive and critical system data sets must not exist on shared DASD.
Legacy ID: V-97845
Legacy ID: SV-106949

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 bel 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), thereby 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-223571
Group Title: SRG-OS-000420-GPOS-00186
Rule ID: SV-223571r853552_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000360
Rule Title: IBM z/OS Policy agent must contain a 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.
Legacy ID: V-97847
Legacy ID: SV-106951

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 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 application and policy agent 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-223572
Group Title: SRG-OS-000142-GPOS-00071
Rule ID: SV-223572r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-000370

Rule Title: 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: V-97849
Legacy ID: SV-106953

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-223573
Group Title: SRG-OS-000028-GPOS-00009
Rule ID: SV-223573r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-002240
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-97851
Legacy ID: SV-106955

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 reauthenticates. No other activity aside from reauthentication must 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: Configure the session manager to retain a user's session lock until that user reestablishes access using established identification and authentication procedures.

CCI: CCI-000056

Group ID (Vulid): V-223574
Group Title: SRG-OS-000363-GPOS-00150
Rule ID: SV-223574r853553_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-002330
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: V-97853
Legacy ID: SV-106957

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-223575
Group Title: SRG-OS-000031-GPOS-00012
Rule ID: SV-223575r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-002350
Rule Title: IBM z/OS must employ a session manager that conceal, via the session lock, information previously visible on the display with a publicly viewable image.
Legacy ID: V-97855
Legacy ID: SV-106959

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-223576
Group Title: SRG-OS-000029-GPOS-00010
Rule ID: SV-223576r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-002360

Rule Title: IBM z/OS must employ a session manager to manage session lock after a 15-minute period of inactivity.
Legacy ID: SV-106961
Legacy ID: V-97857

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 reauthenticates. No other activity aside from reauthentication must 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 initiate 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-223577
Group Title: SRG-OS-000002-GPOS-00002
Rule ID: SV-223577r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-002370
Rule Title: IBM z/OS System Administrator must develop a procedure to automatically remove or disable temporary user accounts after 72 hours.
Legacy ID: SV-106963
Legacy ID: V-97859

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 automatically remove or disable temporary user accounts after 72 hours.

CCI: CCI-000016

Group ID (Vulid): V-223578
Group Title: SRG-OS-000123-GPOS-00064
Rule ID: SV-223578r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-002380
Rule Title: IBM z/OS system administrator must develop a procedure to automatically remove or disable emergency accounts after the crisis is resolved or 72 hours.
Legacy ID: V-97861
Legacy ID: SV-106965

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-223579
Group Title: SRG-OS-000304-GPOS-00121
Rule ID: SV-223579r853554_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-002390
Rule Title: IBM z/OS system administrator must develop a procedure to notify system administrators and ISSOs of account enabling actions.
Legacy ID: V-97863
Legacy ID: SV-106967

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.

Check Content:
Ask the system administrator for the procedure to notify system administrators and ISSOs of account enabling actions.

If no procedures are in place, this is a finding.

Fix Text: Develop and document a procedure to notify system administrators and ISSOs of

account enabling actions.

CCI: CCI-002132

Group ID (Vulid): V-223580
Group Title: SRG-OS-000126-GPOS-00066
Rule ID: SV-223580r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-002410
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: V-97865
Legacy ID: SV-106969

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-223581

Group Title: SRG-OS-000437-GPOS-00194
Rule ID: SV-223581r853555_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-002420
Rule Title: IBM z/OS system administrator must develop a procedure to remove all software components after updated versions have been installed.
Legacy ID: V-97867
Legacy ID: SV-106971

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-223582
Group Title: SRG-OS-000447-GPOS-00201
Rule ID: SV-223582r853556_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-002430
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: V-97869
Legacy ID: SV-106973

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-223583
Group Title: SRG-OS-000030-GPOS-00011
Rule ID: SV-223583r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-002440
Rule Title: IBM z/OS must employ a session manager configured for users to directly initiate a session lock for all connection types.
Legacy ID: V-97871
Legacy ID: SV-106975

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 manage to allow users to directly initiate a session lock for all connection types.

CCI: CCI-000058

Group ID (Vulid): V-223584
Group Title: SRG-OS-000118-GPOS-00060
Rule ID: SV-223584r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-002470
Rule Title: ACF2 system administrator must develop a procedure to disable account identifiers (individuals, groups, roles, and devices) after 35 days of inactivity.
Legacy ID: SV-106977
Legacy ID: V-97873

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:
Ask the system administrator for the procedure to disable account identifiers (individuals, groups, roles, and devices) after 35 days of inactivity.

If there is no procedure this is a finding.

Fix Text: Develop a procedure to disable account identifiers (individuals, groups, roles, and

devices) after 35 days of inactivity.

CCI: CCI-000795

Group ID (Vulid): V-223585
Group Title: SRG-OS-000479-GPOS-00224
Rule ID: SV-223585r853557_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-OS-003430
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-106979
Legacy ID: V-97875

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 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-223586
Group Title: SRG-OS-000032-GPOS-00013
Rule ID: SV-223586r853558_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-SH-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-106981
Legacy ID: V-97877

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 cyber attacks 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:
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-223587
Group Title: SRG-OS-000228-GPOS-00088
Rule ID: SV-223587r533198_rule

Severity: CAT II
Rule Version (STIG-ID): ACF2-SH-000030
Rule Title: IBM z/OS SSH daemon must be configured with the Department of Defense (DoD) logon banner.
Legacy ID: SV-106983
Legacy ID: V-97879

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."

Satisfies: SRG-OS-000228-GPOS-00088, SRG-OS-000023-GPOS-00006

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 s 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 banner below 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 banner below 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-000048

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

Group ID (Vulid): V-223588
Group Title: SRG-OS-000096-GPOS-00050
Rule ID: SV-223588r533198_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-SH-000040
Rule Title: IBM z/OS SSH daemon must be configured to only use the SSHv2 protocol.
Legacy ID: SV-106985
Legacy ID: V-97881

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, 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 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-223589
Group Title: SRG-OS-000033-GPOS-00014
Rule ID: SV-223589r918616_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-SH-000050
Rule Title: IBM z/OS SSH daemon must be configured to use a FIPS 140-2 compliant cryptographic algorithm.
Legacy ID: V-97883
Legacy ID: SV-106987

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

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.

Configure for message authentication to MACs "hmac-sha1" or greater.

Edit the z/OS-specific sshd server system-wide configuration file configuration as follows:
FIPSMODE=YES
CiphersSource=ICSF
MACsSource=ICSF

CCI: CCI-000068

CCI: CCI-000803

CCI: CCI-001453

Group ID (Vulid): V-223590
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223590r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-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-97885
Legacy ID: SV-106989

Vulnerability Discussion: HFS directories and files of the Syslog daemon provide the configuration and executable properties of this product. Failure to properly secure these objects could lead to unauthorized access. This exposure may result in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

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 is as below, this is not a finding.

/usr/sbin/syslogd 1740 fff

Enter:
cd /etc/
Enter
ls -alW

If the 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: With the assistance of a systems programmer with UID(0) and/or SUPERUSER access, review the UNIX permission bits and user audit bits on the HFS directories and files for the Syslog daemon. Ensure they 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-223591
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223591r533198_rule

Severity: CAT II
Rule Version (STIG-ID): ACF2-SL-000020
Rule Title: IBM z/OS Syslog daemon must be started at z/OS initialization.
Legacy ID: V-97887
Legacy ID: SV-106991

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) to ensure the Syslog daemon is automatically started 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-223592
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223592r836663_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-SL-000030
Rule Title: IBM z/OS Syslog daemon must be properly defined and secured.
Legacy ID: V-97889
Legacy ID: SV-106993

Vulnerability Discussion: The Syslog daemon, known as syslogd, is a zOS UNIX daemon that provides a central processing point for log messages issued by other zOS UNIX processes. It is also possible to receive log messages from other network-connected hosts. Some of the IBM Communications Server components that may send messages to syslog are the FTP, TFTP, zOS UNIX Telnet, DNS, and DHCP servers. The messages may be of varying importance levels including general process information, diagnostic information, critical error notification, and audit-class information. Primarily because of the potential to use this information in an audit process, there is a security interest in protecting the syslogd process and its associated data.

The Syslog daemon requires special privileges and access to sensitive resources to provide its system services. Failure to properly define and control the Syslog daemon could lead to unauthorized access. This exposure may result in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Check Content:
The syslog daemon is defined as SYSLOGD.

From the ACF command screen enter:
SET LID
LIST SYSLOGD

If the Syslog daemon is not defined, this is a finding.

If the SYSLOGD logonid is not defined with the STC attribute, this is a finding.

If the SYSLOGD userid has UID(0), HOME('/'), and PROGRAM('/bin/sh') specified in the OMVS segment, this is not a finding.

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.

Fix Text: Define the Syslog daemon logonid as SYSLOGD with the STC attribute.

To set up and use as an MVS Started Proc, the following sample commands are provided:
SET LID

INSERT SYSLOGD NAME(SYSLOGD STC) GROUP(stctcpx) STC

The SYSLOGD userid has UID(0), HOME('/'), and PROGRAM('/bin/sh') specified in the OMVS segment.

SET PROFILE(USER) DIVISION(OMVS)
INSERT SYSLOGD UID(0) HOME(/) PROGRAM(/bin/sh)

F ACF2,REBUILD(USR),CLASS(P)

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-223593
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223593r836696_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-SM-000010
Rule Title: IBM z/OS DFSMS resource class(es) must be defined to the GSO CLASMAP record in accordance with security requirements.
Legacy ID: V-97891
Legacy ID: SV-106995

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.

The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any one of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during a migration process or contingency plan activation.

Check Content:
From the ISPF Command Shell enter:
ACF
SET CONTROL(GSO)
SHOW CLASMAP

If both MGMTCLAS and STORCLAS resource classes are uniquely defined (i.e., not type SAF), this is not a finding.

Fix Text: Define the GSO CLASMAP record with the following definitions:

MGMTCLAS
STORCLAS

Ensure both resource classes above are defined uniquely.

Example:
SHOW SAFDEF

SET CONTROL(GSO)
INSERT CLASMAP.MGMTCLAS RESOURCE(MGMTCLAS) RSRCTYPE(MGM)
ENTITYTLN(8)
INSERT CLASMAP.STORCLAS RESOURCE(STORCLAS) RSRCTYPE(STR)
ENTITYTLN(8
F ACF2,REFRESH(ALL)

CCI: CCI-000213

Group ID (Vulid): V-223594
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223594r861179_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-SM-000020
Rule Title: IBM z/OS DFSMS Program Resources must be properly defined and protected.
Legacy ID: SV-106997
Legacy ID: V-97893

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 load modules residing in the following Load libraries to determine Program resource definitions:
SYS1.DGTLLIB for DFSMSdfp/ISMF
SYS1.DGTLLIB for DFSMSdss/ISMF
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 ACF2 resources are defined with a default access of NONE, this is not a finding.

If the ACF2 resource access authorizations restrict access to the appropriate personnel, this is not a finding.

Refer to the chapter titled 'Protecting the Storage Management Subsystem' in the IBM z/OS DFSMSdfp Storage Administration Guide to assist with guidance on appropriate access.

Fix Text: 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.

Refer to the chapter titled "Protecting the Storage Management Subsystem" in the IBM z/OS DFSMSdfp Storage Administration Guide.

Use SMS Program Resources tables to determine the resources, access requirements for SMS Program Resources. Ensure the guidelines for the resource type, resources, and/or generic equivalent specified.

The ACF2 resources as designated in the above table are defined with a default access of PREVENT.

The ACF2 resource access authorizations restrict access to the appropriate personnel as designated in the above tables.

The following commands are provided as a sample for implementing resource controls:
$KEY(ACBFUTO2) TYPE(PGM)
UID(********) ALLOW
UID(*) PREVENT

F ACF2,REBUILD(PGM)

CCI: CCI-000213

Group ID (Vulid): V-223595
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223595r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-SM-000030
Rule Title: IBM z/OS DFSMS control data sets must be protected in accordance with security requirements.
Legacy ID: SV-106999
Legacy ID: V-97895

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 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 ACF2 data set rules for the SCDS, ACDS, COMMDS, and ACS data sets restrict UPDATE and ALLOCATE access to only systems programming personnel, this not is a finding.

If the ACF2 data set rules for the SCDS, ACDS, COMMDS, and ACS data sets do not restrict UPDATE and ALLOCATE 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: Configure DFSMS control data sets to restrict UPDATE or ALLOCATE access to system programmers responsible for DASD management. Justification is required for any additional access.

Review the SYS1.PARMLIB(IGDSMSxx) data set 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

Define ACF2 data set rules for the SCDS, ACDS, COMMDS, and ACS data sets to restrict UPDATE and ALLOCATE access to only systems programming personnel.

Note: At the discretion of the ISSM, DASD administrators are allowed UPDATE access to the control data sets.

Example:
$KEY(S3D)
$PREFIX(SYS3)
DFSMS.MVA.ACDS UID(uuuuuuuu) R(A) W(L) A(L) E(A)

CCI: CCI-000213

Group ID (Vulid): V-223596
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223596r533198_rule

Severity: CAT II
Rule Version (STIG-ID): ACF2-SM-000040
Rule Title: IBM z/OS DFMSM resource class(es)must be defined to the GSO SAFDEF record in accordance with security requirements.
Legacy ID: SV-107001
Legacy ID: V-97897

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:
ACF
SET CONTROL(GSO)
SHOW SAFDEF

If both FACILITY and PROGRAM resource classes are defined, this is not a finding.

Fix Text: Define the GSO SAFDEF record with the following definitions:

FACILITY
PROGRAM

Ensure both resource classes above are defined.

Example:
SHOW SAFDEF

SET C(GSO)
INSERT SAFDEF.FAC FUNCRET(4) FUNCRSN(0) ID(FACILITY) MODE(GLOBAL)
RACROUTE(REQUEST=AUTH CLASS=FACILITY) RETCODE(4)

F ACF2,REFRESH(ALL)

CCI: CCI-000213

Group ID (Vulid): V-223597
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223597r861189_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-SM-000050
Rule Title: IBM z/OS DFSMS resources must be protected in accordance with the proper security requirements.
Legacy ID: SV-107003
Legacy ID: V-97899

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:
ACF
SET RESOURCE(FAC)
SET VERBOSE
LIST LIKE(STG-)

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

The resource rule for FACILITY (FAC) $KEY(STGADMIN) has a default access of PREVENT.

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 resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE is defined with access of PREVENT.

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 = PREVENT.

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: Configure access requirements for SMS Resources as follows. Define the guidelines to ensure the resource type, resources, and/or generic equivalent are followed.

(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.)

The ACF2 resources are defined with a default access of PREVENT.

Ensure that the following items are in effect:

Ensure that no access is given to the high-level STGADMIN resource.

Example:
$KEY(STGADMIN) TYPE(FAC)
- UID(*) PREVENT

Ensure no access is given to resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE.

Example:
$KEY(STGADMIN) TYPE(FAC)
IGG.STGADMIN.IGG.CATALOG.SECURITY.CHANGE-UID(*) PREVENT
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 = PREVENT

The STGADMIN.DPDSRN.olddsname is restricted to System Programmers and all access is logged.

Example:
$KEY(STGADMIN) TYPE(FAC)

DPDSRN.- UID(sysprgmr) SERVICE(READ) LOG
DPDSRN.- UID(*) PREVENT

The STGADMIN.IGD.ACTIVATE.CONFIGURATION is restricted to System Programmers and all access is logged.

Example:
$KEY(STGADMIN) TYPE(FAC)
IGD.ACTIVATE.CONFIGURATION UID(sysprgmr) SERVICE(READ) LOG
IGD.ACTIVATE.CONFIGURATION UID(*) PREVENT

The STGADMIN.IGG.DEFDEL.UALIAS is restricted to System Programmers and Security personnel and all access is logged.

Example:
$KEY(STGADMIN) TYPE(FAC)
IGG.DEFDEL.UALIAS UID(seca) SERVICE(READ) LOG
IGG.DEFDEL.UALIAS UID(secd) SERVICE(READ) LOG
IGG.DEFDEL.UALIAS UID(sysprgmr) SERVICE(READ) LOG
IGG.DEFDEL.UALIAS UID(*) PREVENT

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

Example:
$KEY(STGADMIN) TYPE(FAC)
ADR.COPY.CNCURRNT.- UID(endusers) SERVICE(READ)

The following resource is restricted to Application Production Support Team members, Automated Operations, DASD managers, and System programmers.

STGADMIN.IDC.DCOLLECT

Example:
$KEY(STGADMIN) TYPE(FAC)
IDC.DCOLLECT.- UID(apps) SERVICE(READ)
IDC.DCOLLECT.- UID(auto) SERVICE(READ)
IDC.DCOLLECT.- UID(dasb) SERVICE(READ)

IDC.DCOLLECT.- UID(dasd) SERVICE(READ)
IDC.DCOLLECT.- UID(sysprgmr) SERVICE(READ)
IDC.DCOLLECT.- UID(*) PREVENT

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

Example:
$KEY(STGADMIN) TYPE(FAC)
ARC.CANCEL.- UID(apps) SERVICE(READ)
ARC.CANCEL.- UID(dasb) SERVICE(READ)
ARC.CANCEL.- UID(dasd) SERVICE(READ)
ARC.CANCEL.- UID(sysprgmr) SERVICE(READ)
ARC.CANCEL.- UID(*) PREVENT

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:
$KEY(STGADMIN) TYPE(FAC)
ADR. - UID(dasb) SERVICE(READ)
ADR.- UID(dasd) SERVICE(READ)
ADR.- UID(sysprgmr) SERVICE(READ)
ADR.- UID(*) PREVENT

The following Storage Administrator functions prefix is restricted to DASD managers and System programmers and all access is logged.

STGADMIN.ADR.STGADMIN.

Example:
$KEY(STGADMIN) TYPE(FAC)
ADR.STGADMIN.- UID(dasb) SERVICE(READ) LOG
ADR.STGADMIN.- UID(dasd) SERVICE(READ) LOG
ADR.STGADMIN.- UID(sysprgmr) SERVICE(READ) LOG
ADR.STGADMIN.- UID(*) PREVENT

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223598
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223598r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-SM-000060
Rule Title: IBM z/OS using DFSMS must properly specify SYS(x).PARMLIB(IGDSMSxx), SMS parameter settings.
Legacy ID: SV-107005
Legacy ID: V-97901

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-223599
Group Title: SRG-OS-000032-GPOS-00013
Rule ID: SV-223599r861181_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-TC-000010
Rule Title: IBM z/OS PROFILE.TCPIP configuration statements for the TCP/IP stack must be coded properly.
Legacy ID: V-97903
Legacy ID: SV-107007

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 cyber attacks 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.

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 the SMFPARMS statement is not coded or commented out, this is not a finding.

If the DELETE statement is not coded or commented out for production system, this is not a finding.

If the SMFCONFIG statement is coded with (at least) the FTPCLIENT and TN3270CLIENT operands, this is not a finding.

If the TCPCONFIG and UDPCONFIG statements are coded with (at least) the RESTRICTLOWPORTS operand, this is not a finding.

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: Configure the statements in the PROFILE.TCPIP file 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 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.

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-223600
Group Title: SRG-OS-000297-GPOS-00115
Rule ID: SV-223600r853560_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-TC-000020
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: V-97905
Legacy ID: SV-107009

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-223601

Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223601r861182_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-TC-000030
Rule Title: IBM z/OS TCP/IP resources must be properly protected.
Legacy ID: V-97907
Legacy ID: SV-107011

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 ACF command screen enter:
SET RESOURCE(SER)
SET VERBOSE
The SERVAUTH resource class is mapped to the standard resource type SER.
LIST LIKE (-)

If no access is given to the EZA, EZB, and IST high level resources of the SERVAUTH resource class, and default access of PREVENT is specified, this is not a finding.

If the product CSSMTP is on the system, no access is given to EZB.CSSMTP of the SERVAUTH resource class, this is not a finding.

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 email 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.

If the EZB.STACKACCESS. resource access authorizations restrict access to those started tasks with valid requirements and users with valid FTP access requirements, this is not a finding.

If 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, this is not a finding.

If 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, this is not a finding.

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.)

The SERVAUTH resource class is mapped to the required resource type SER.

Ensure that the EZA, EZB, and IST resources are defined to the SERVAUTH resource class with a default access of PREVENT.

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 email 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:

$KEY(EZB) TYPE(SER)
- UID(*) PREVENT
CSSMTP. - UID(*) PREVENT
CSSMTP.sysname.writername.JESnode UID(authusers) SERVICE(READ) ALLOW
FTP.- UID(authusers) SERVICE(READ) ALLOW
FTP.sysname.ftpstc.ACCESS.HFS UID(ftpprofile) SERVICE(READ) ALLOW
NETACCESS.- UID(authusers) SERVICE(READ) ALLOW
PORTACCESS.- UID(authusers) SERVICE(READ) ALLOW
STACKACCESS.- UID(authusers) SERVICE(READ) ALLOW
STACKACCESS.sysname.TCPIP UID(ftpprofile) SERVICE(READ) ALLOW
INITSTACK.- UID(authusers) SERVICE(READ) ALLOW

COMPILE 'ACF2.MVA.SER(EZB)' STORE

F ACF2,REBUILD(SER)

CCI: CCI-000213

Group ID (Vulid): V-223602
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223602r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-TC-000040
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-97909
Legacy ID: SV-107013

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-223603
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223603r767690_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-TC-000050
Rule Title: IBM z/OS data sets for the Base TCP/IP component must be properly protected.
Legacy ID: V-97911
Legacy ID: SV-107015

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:
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.

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.

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-223604
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223604r768719_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-TC-000060
Rule Title: IBM z/OS Configuration files for the TCP/IP stack must be properly specified.
Legacy ID: V-97913
Legacy ID: SV-107017

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.

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.

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.

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.

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.

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-223605
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223605r836666_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-TC-000070
Rule Title: IBM z/OS Started tasks for the Base TCP/IP component must be defined in accordance with security requirements.
Legacy ID: V-97915
Legacy ID: SV-107019

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:
Verify Logonid(s) assigned to the TCP/IP address space(s), are named TCPIP or, in the case of multiple instances, are prefixed with TCPIP.

From an ACF Command screen enter:
SET LID
LIST LIKE(TCPIP-)

If each TCP/IP logonid its defined with STC, MUSASS, and NO-SMC attributes, this is not a finding.

From the ACF Command screen enter:
SET LID
LIST LIKE(TCPIP-) PROFILE(OMVS)

If the z/OS UNIX attributes are UID(0), HOME directory '/', shell program /bin/sh, this is not a finding.

From an ACF Command screen enter:
SET LID
LIST EZAZSSI

If THE EZAZSSI logonid is defined with STC attribute, this is not a finding.

From the ACF Command screen enter:
SET LID
LIST EZAZSSI PROFILE(OMVS)

If the z/OS UNIX attributes are UID(0), HOME directory '/', shell program /bin/sh, this is not a finding.

Fix Text: Define the Started tasks for the Base TCP/IP component user accounts with the following characteristics:

Named TCPIP or, in the case of multiple instances, prefixed with TCPIP
Defined with the STC, MUSASS, and NO-SMC attributes
z/OS UNIX attributes: UID(0), HOME directory '/', shell program /bin/sh

Named EZAZSSI
Defined with the STC attribute
z/OS UNIX attributes: UID(non-zero), HOME directory '/', shell program /bin/sh

Review the TCP/IP started task accounts, privileges, and access authorizations defined to the ACP. Ensure they conform to the requirements as outlined below.

The following commands can be used to create the user accounts that are required for the TCP/IP address space and the EZAZSSI started task:

SET LID
INSERT TCPIP NAME(TCPIP) GROUP(STCTCPX) STC MUSASS NO-SMC
INSERT EZAZSSI NAME(EZAZSSI) GROUP(STCTCPX) STC

SET PROFILE(USER) DIVISION(OMVS)
INSERT TCPIP UID(0) HOME(/) OMVSPGM(/bin/sh)
INSERT EZAZSSI UID(non-zero) HOME(/) OMVSPGM(/bin/sh)

F ACF2,REBUILD(USR),CLASS(P)

NOTE: At eTrust CA-ACF2 6.4 and above, the PROGRAM field in the user profile record has been renamed to OMVSPGM.

The following additions to the indicated rule sets can be used to assign the privileges that are required for the TCP/IP address space:

$KEY(BPX) TYPE(FAC)
...
DAEMON UID(TCPIP-uid) SERVICE(READ) ALLOW

If the z/OS host machine has hardware encryption installed and enabled, resources owned by the Integrated Cryptographic Service Facility (ICSF) component have been defined. The following rule set additions are required to allow the TN3270 Telnet Server process to access the ICSF resources.

- $KEY(CSFCKI) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- $KEY(CSFCKM) TYPE(CSF)

- UID(TCPIP-uid) SERVICE(READ) ALLOW
- $KEY(CSFDEC) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- $KEY(CSFENC) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- $KEY(CSFOWH) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- $KEY(CSFRNG) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- $KEY(CSFPKB) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- $KEY(CSFPKX) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- $KEY(CSFPKE) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- $KEY(CSFPKD) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- $KEY(CSFPKI) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- $KEY(CSFDSG) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW
- $KEY(CSFDSV) TYPE(CSF)
- UID(TCPIP-uid) SERVICE(READ) ALLOW

The following operator commands are required to complete the updates:
F ACF2,REBUILD(FAC)
F ACF2,REBUILD(CSF)

These commands and definitions assume that the default type code for CSFSERV resources is CSF.

CCI: CCI-000764

Group ID (Vulid): V-245535
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-245535r768734_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-TC-000090
Rule Title: IBM z/OS TCPIP.DATA configuration statement must contain the DOMAINORIGIN or DOMAIN specified for each TCP/IP defined.
Legacy ID: SV-107023
Legacy ID: V-97919

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 configuration statements specified in the TCP/IP Data configuration file guidance are true, this is not a finding.

DOMAINORIGIN/DOMAIN (The DOMAIN statement is functionally equivalent to the DOMAINORIGIN Statement)

Fix Text: Configure the TCPIP.DATA file to include the following:

DOMAINORIGIN/DOMAIN - Specifies the default domain name used for DNS searches.

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-252547
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-252547r816937_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-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:
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-223608
Group Title: SRG-OS-000279-GPOS-00109
Rule ID: SV-223608r853561_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-TN-000010
Rule Title: IBM z/OS PROFILE.TCPIP configuration INACTIVITY statement must be configured to 900 seconds.
Legacy ID: SV-107025
Legacy ID: V-97921

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:
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 PROFILE.TCPIP file as 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.

TELNETPARMS Block (one defined for each port the server is listening to, typically ports 23 and 992)

The TELNETPARMS INACTIVE statement is coded within each TELNETPARMS statement block and specifies a value between 1 and 900.

INACTIVE statements should not be coded with a value greater than 900 or 0. 0 disables the inactivity timer check.

NOTE: Effective in z/OS release 1.2, the INACTIVE statement can appear in both TELNETGLOBAL and TELNETPARM statement blocks.

CCI: CCI-002361

Group ID (Vulid): V-223609
Group Title: SRG-OS-000392-GPOS-00172
Rule ID: SV-223609r853562_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-TN-000020
Rule Title: IBM z/OS SMF recording options for the TN3270 Telnet Server must be properly specified.
Legacy ID: SV-107027
Legacy ID: V-97923

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 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.

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.

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: Effective in z/OS release 1.2, the SMFINIT and SMFTERM statement can appear in both TELNETGLOBAL and TELNETPARM statement blocks.

Fix Text: Configure the TELNETPARMS SMFINIT and SMFTERM statements in the PROFILE.TCPIP file to conform 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-223610
Group Title: SRG-OS-000033-GPOS-00014
Rule ID: SV-223610r877398_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-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-97925
Legacy ID: SV-107029

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-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 that 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-223611
Group Title: SRG-OS-000023-GPOS-00006

Rule ID: SV-223611r864504_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-TN-000040
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-97927
Legacy ID: SV-107031

Vulnerability Discussion: A logon banner can be used to inform users about the environment during the initial logon. In the DISA environment, logon banners are used to warn users against unauthorized entry and the possibility of legal action for unauthorized users, and advise all users that system use constitutes consent to monitoring. Failure to display a logon warning banner without this type of information could adversely impact the ability to prosecute unauthorized users and users who abuse the system.

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 TCPIP 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-223613
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223613r861183_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-TN-000060
Rule Title: IBM z/OS VTAM session setup controls for the TN3270 Telnet Server must be properly specified.
Legacy ID: V-97931
Legacy ID: SV-107035

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 into 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 following 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-223614
Group Title: SRG-OS-000163-GPOS-00072
Rule ID: SV-223614r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-TN-000070
Rule Title: IBM z/OS PROFILE.TCPIP configuration for the TN3270 Telnet Server must have INACTIVE statement properly specified.
Legacy ID: V-97933
Legacy ID: SV-107037

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.

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 PROFILE.TCPIP file as 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.

"TELNETPARMS Block (one defined for each port the server is listening to, typically ports 23 and 992)"

The TELNETPARMS INACTIVE statement is coded within each TELNETPARMS statement block and specifies a value between 1 and 900.

INACTIVE statements should not be coded with a value greater than 900 or 0. 0 disables the inactivity timer check.

NOTE: Effective in z/OS release 1.2, the INACTIVE statement can appear in both TELNETGLOBAL and TELNETPARM statement blocks.

CCI: CCI-001133

Group ID (Vulid): V-223615
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223615r861184_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-TS-000010
Rule Title: IBM z/OS TSOAUTH resources must be restricted to authorized users.
Legacy ID: SV-107039
Legacy ID: V-97935

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:
ACF
SET RESOURCE(TSO)
SET VERBOSE
LIST LIKE(-)

If the ACCT authorization is restricted to security personnel, this is not a finding.

If 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, this is not a finding.

If the MOUNT authorization is restricted to DASD batch users only, this is not a finding.

If the OPER authorization is restricted to authorized systems personnel (e.g., systems programming personnel, operations staff, etc), this is not a finding.

If the PARMLIB authorization is restricted to only z/OS systems programming personnel and READ access may be given to auditors, this is not a finding.

If the TESTAUTH authorization is restricted to only z/OS systems programming personnel, this is not a finding.

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-223616
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223616r533198_rule
Severity: CAT I
Rule Version (STIG-ID): ACF2-US-000010
Rule Title: IBM z/OS UNIX SUPERUSER resource must be protected in accordance with guidelines.
Legacy ID: SV-107041
Legacy ID: V-97937

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:
ACF
RESOURCE(UNI)
LIST LIKE(SUPER-)

If the ACF2 rules for the SUPERUSER resource specify a default access of NONE, this is not a finding.

If there are no ACF2 rules that allow access to the SUPERUSER resource, this is not a finding.

If there is no ACF2 rule for CHOWN.UNRESTRICTED defined, this is not a finding.

If the ACF2 rules for each of the SUPERUSER resources listed in the z/OS UNIX System Services Planning, Establishing UNIX Security, specify a default access of NONE, this is not a finding.

If the ACF2 rules for each of the SUPERUSER resources listed in the UNIXPRIV CLASS RESOURCES Table in the z/OS UNIX System Services Planning, Establishing UNIX Security, restrict access to appropriate system tasks or systems programming personnel, this is not a finding.

Fix Text: Configure ACF2 SUPERUSER resources for the UNIXPRIV resource class to restrict to appropriate system tasks and/or system programming personnel.

Configure the ACF2 rules for the SUPERUSER resource to specify a default access of NONE.

Configure no ACF2 rules that allow access to the SUPERUSER resource.

Configure no ACF2 rule for CHOWN.UNRESTRICTED defined.

Configure the ACF2 rules for each of the SUPERUSER resources listed in the UNIXPRIV CLASS RESOURCES Table in the z/OS UNIX System Services Planning, Establishing UNIX security to specify a default access of NONE.

Configure the ACF2 rules for each of the SUPERUSER resources listed in the UNIXPRIV CLASS RESOURCES Table in the z/OS UNIX System Services Planning, Establishing UNIX security to restrict access to appropriate system tasks or systems programming personnel.

Example:
SET R(UNI)
$KEY(SUPERUSER) TYPE(UNI)
$MEMBER(SUPRUSER)
FILESYS UID(sysprgmr LOG
FILESYS.CHOWN UID(sysprgmr) LOG
FILESYS.MOUNT UID(sysprog) LOG
FILESYS.PFSCTL UID(sysprgmr) LOG
FILESYS.VREGISTER UID(sysprgmr) LOG
IPC.RMID UID(sysprgmr) LOG
PROCESS.GETPSENT UID(sysprgmr) LOG
PROCESS.KILL UID(sysprgmr) LOG
PROCESS.PTRACE UID(sysprgmr) LOG
SETPRIORITY UID(sysprgmr) LOG
- UID(*) PREVENT

CCI: CCI-000213

Group ID (Vulid): V-223617
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223617r861185_rule
Severity: CAT II

Rule Version (STIG-ID): ACF2-US-000020
Rule Title: IBM z/OS UNIX security parameters in etc/profile must be properly specified.
Legacy ID: SV-107043
Legacy ID: V-97939

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/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-223618
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223618r861186_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000030
Rule Title: IBM z/OS UNIX security parameters in /etc/rc must be properly specified.
Legacy ID: SV-107045
Legacy ID: V-97941

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/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

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: 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 below.
-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.

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.

CCI: CCI-000213

Group ID (Vulid): V-223619
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223619r853564_rule

Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000040
Rule Title: IBM z/OS UNIX resources must be protected in accordance with security requirements.
Legacy ID: SV-107047
Legacy ID: V-97943

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:
ACF
SET RESOURCE(SUR)
SET VERBOSE
LIST LIKE(BPX-)

If the ACF2 rules for all BPX.SRV.user TYPE(SUR) resources specify a default access of NONE, this is not a finding.

If the ACF2 rules for all BPX.SRV.user TYPE(SUR) resources restrict access to system software processes (e.g., web servers) that act as servers under z/OS UNIX, this is not a finding.

If the ACF2 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: Configure BPX. SRV.userid resources to be properly protected and access 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.

The default access for each BPX.SRV.userid resource must be no access. Access can be permitted only to system software processes that act as servers under OS/390 UNIX (e.g., web servers) and users whose access an approval are identified in the Site Security Plan.

Example:
SET R(SUR)
$KEY(BPX) TYPE(SUR)
SRV.INTERNAL UID(FJB****STC******IMWEBSRV) SERVICE(READ) LOG
SRV.PRIVATE UID(FJB****STC******IMWEBSRV) SERVICE(READ) LOG
SRV.PUBLIC UID(FJB****STC******IMWEBSRV) SERVICE(READ) LOG
SRV.WEBADM UID(FJB****STC******IMWEBSRV) SERVICE(READ) LOG
- UID(*) PREVENT

CCI: CCI-000213

CCI: CCI-002233

Group ID (Vulid): V-223620
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223620r861187_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000050
Rule Title: IBM z/OS UNIX MVS HFS directory(s) with other write permission bit set must be properly defined.
Legacy ID: V-97945
Legacy ID: SV-107049

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:
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, this is not a 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-223621
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223621r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000060

Rule Title: IBM z/OS BPX resource(s) must be protected in accordance with security requirements.
Legacy ID: V-97947
Legacy ID: SV-107051

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:
ACF
SET RESOURCE(FAC)
SET VERBOSE
LIST LIKE(BPX-)

If the ACF2 rules for the BPX resource specify a default access of NONE, this is not a finding.

If there are no ACF2 rules that allow access to the BPX resource, this is not a finding.

If there is no ACF2 rule for BPX.SAFFASTPATH defined, this is not a finding.

If the ACF2 rules for each of the BPX resources listed in z/OS UNIX System Services Planning, Establishing UNIX security, specify a default access of NONE, this is not a finding.

If the ACF2 rules for each of the BPX resources listed in the in z/OS UNIX System Services Planning, Establishing UNIX security, restrict access to appropriate system tasks or systems programming personnel, this is not a finding.

Fix Text: Configure BPX. Resources to be properly protected and access is restricted to appropriate system tasks or systems programming personnel.

Configure the following items for the FACILITY resource class, TYPE(FAC):

The ACF2 rules for the BPX resource specify a default access of NONE.

Example:
$KEY(BPX) TYPE(FAC)
- UID(*) PREVENT

There are no ACF2 rules that allow access to the BPX resource.

Example:
$KEY(BPX) TYPE(FAC)
- UID(*) PREVENT

There is no ACF2 rule for BPX.SAFFASTPATH defined.

Example:
$KEY(BPX) TYPE(FAC)
SAFFASTPATH UID(*) PREVENT

The ACF2 rules for each of the BPX resources listed in the General Facility Class BPX Resources Table, in the z/OS UNIX System Services Planning, Establishing UNIX security, specify a default access of NONE.

Example:
$KEY(BPX) TYPE(FAC)
DAEMON UID(*) PREVENT
DEBUG UID(*) PREVENT
FILEATTR.APF UID(*) PREVENT
FILEATTR.PROGCTL UID(*) PREVENT
JOBNAME UID(*) PREVENT
SAFFASTPATH UID(*) PREVENT
SERVER UID(*) PREVENT
SMF UID(*) PREVENT
STOR.SWAP UID(*) PREVENT
SUPERUSER UID(*) PREVENT
WLMSERVER UID(*) PREVENT

The ACF2 rules for each of the BPX resources listed in the 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 as specified.

Example:
$KEY(BPX) TYPE(FAC)
DAEMON UID(*******STC******FTPD) SERVICE(READ) LOG
DAEMON UID(*******STC******INETD) SERVICE(READ) LOG

DAEMON UID(*******STC******NAMED) SERVICE(READ) LOG
DAEMON UID(*******STC******OMVSKERN) SERVICE(READ) LOG
DAEMON UID(*******STC******OMVS) SERVICE(READ) LOG
DAEMON UID(*******STC******OROUTED) SERVICE(READ) LOG
DAEMON UID(*******STC******OSNMPD) SERVICE(READ) LOG

CCI: CCI-000213

Group ID (Vulid): V-223622
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223622r861188_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000070
Rule Title: IBM z/OS UNIX SYSTEM FILE SECURITY SETTINGS must be properly protected or specified.
Legacy ID: V-97949
Legacy ID: SV-107053

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 must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Access enforcement mechanisms include access control lists, access control matrices, and cryptography.

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/tablename 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/tablename 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-223623
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223623r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000080
Rule Title: IBM z/OS UNIX MVS data sets with z/OS UNIX components must be properly protected.
Legacy ID: V-97951
Legacy ID: SV-107055

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.

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 UPDATE and ALLOCATE 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 UPDATE and ALLOCATE access to systems programming personnel.

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.

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.

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-223624
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223624r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000090
Rule Title: IBM z/OS UNIX MVS data sets or HFS objects must be properly protected.
Legacy ID: V-97953
Legacy ID: SV-107057

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

must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

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 sets referenced in the ROOT and the MOUNT statements in BPXPRMxx restrict update and/or allocate 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 update and/or allocate access to systems programming personnel.

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-223625
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223625r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000100
Rule Title: IBM z/OS UNIX HFS permission bits and audit bits for each directory must be properly protected.
Legacy ID: V-97955
Legacy ID: SV-107059

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

Check Content:
From the ISPF Command Shell enter:
omvs
cd /
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 Tale below, this is not a finding.

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 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 each of the HFS directory in the table below to be equal or more restrictive.

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 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 0755 /
chaudit w=sf,rx+f /
chmod 0755 /bin
chaudit rwx=f /bin

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-223626
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223626r918619_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000110
Rule Title: IBM z/OS UNIX MVS data sets used as step libraries in /etc/steplib must be properly protected.
Legacy ID: SV-107061
Legacy ID: V-97957

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 STEPLIBLIST statement in the BPXPRMxx member of PARMLIB.

If the STEPLIBLIST points to an etc/steplib, go to the ISPF Command Shell and enter:
OMVS
cd /etc
cat <filename>

If the ESM data set rules for libraries specified in the STEPLIBLIST file do not restrict WRITE and/or ALLOCATE access to only systems programming personnel, this is a finding.

If the ESM data set rules for libraries specified in the STEPLIBLIST file do not specify that all (i.e., failures and successes) WRITE and/or ALLOCATE access will be logged, this is a finding.

Fix Text: Define the STEPLIBLIST with update and allocate access to libraries residing in the /etc/steplib limited to systems programmers only.

The STEPLIBLIST parameter specifies the pathname of the HFS file that contains the list of MVS data sets used as step libraries for programs that have the set-user-id or set group id permission bit set.

The use of STEPLIBLIST is at the site's discretion, but if used, the value of STEPLIBLIST will be /etc/steplib. All WRITE and ALLOCATE access to the MVS data sets in the list will be logged and only systems programming personnel will be authorized to update the data sets.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223628
Group Title: SRG-OS-000259-GPOS-00100
Rule ID: SV-223628r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000130

Rule Title: IBM z/OS UNIX HFS permission bits and audit bits for each directory must be properly protected or specified.
Legacy ID: SV-107065
Legacy ID: V-97961

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 must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Check Content:
From the ISPF Command Shell enter:
omvs
cd /
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 table below, this is not a finding.

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 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 each of the HFS directory in the table below to be equal or more restrictive.

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 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 0755 /
chaudit w=sf,rx+f /
chmod 0755 /bin
chaudit rwx=f /bin

CCI: CCI-001499

Group ID (Vulid): V-223629
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223629r861190_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000140
Rule Title: IBM z/OS UNIX OMVS parameters in PARMLIB must be properly specified.
Legacy ID: SV-107067
Legacy ID: V-97963

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 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-223630
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223630r861191_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000150
Rule Title: IBM z/OS UNIX HFS MapName files security parameters must be properly specified.
Legacy ID: SV-107069
Legacy ID: V-97965

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.

The organization must perform a periodic scan/review of the application (as required by CCI-000384) and disable functions, ports, protocols, and services deemed to be unneeded or non-secure.

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-223631
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-223631r864507_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000160
Rule Title: IBM z/OS UNIX BPXPRMxx security parameters in PARMLIB must be properly

specified.
Legacy ID: V-97967
Legacy ID: SV-107071

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:
Refer to the proper BPXPRMxx member in 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 NOSETUID
SETUID (for Vendor-provided files)
SECURITY
STARTUP_PROC OMVS

CCI: CCI-000366

Group ID (Vulid): V-223632
Group Title: SRG-OS-000096-GPOS-00050
Rule ID: SV-223632r858912_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000170
Rule Title: IBM z/OS User exits for the FTP Server must not be used without proper approval and documentation.
Legacy ID: V-97969
Legacy ID: SV-107073

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.

Several user exit points in the FTP Server component are available to permit customization of its operating behavior. These exits can be used to modify functions such as FTP command usage, client connection controls, post processing tasks, and SMF record modifications. Without proper review and adequate documentation of these exit programs, undesirable operations and degraded security may result. This exposure could lead to unauthorized access impacting data integrity or the availability of some system services, or contribute to the loss of accountability and hamper security audit activities.

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.

If the following items are in effect for FTP Server user exits, this is not a finding:

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.

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-223633
Group Title: SRG-OS-000096-GPOS-00050
Rule ID: SV-223633r695457_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-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-97971
Legacy ID: SV-107075

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 unless justified and documented with the ISSO, 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 ESM and it may require a UID(0) (i.e., superuser authority) value.

CCI: CCI-000382

Group ID (Vulid): V-223634
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223634r861192_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000190
Rule Title: IBM z/OS user account for the z/OS UNIX SUPERSUSER userid must be properly defined.
Legacy ID: V-97973
Legacy ID: SV-107077

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:
SET LID
LIST LIKE (superuser userid)

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

From an ACF command input screen enter:
SET PROFILE(USER) DIVISION(OMVS)
SET VERBOSE
LIST <superuser userid>

If the SUPERUSER userid is defined as follows, this is not a finding:
- 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-223635
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223635r861193_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000200
Rule Title: IBM z/OS UNIX user accounts must be properly defined.
Legacy ID: V-97975
Legacy ID: SV-107079

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 an ACF Command screen enter:

SET PROFILE(USER) DIV(OMVS)

LI LIKE(-)

If each user account is defined as follows this is not a finding.
A unique UID number (except for UID(0) users)
Use the following as a quick test for duplicate UIDs apart from UID 0

SHOW OMVS USERS(1-2147483647) DUPLICATES

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: Define any z/OS UNIX user as follows:
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-223636
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223636r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000210
Rule Title: IBM z/OS UNIX groups must be defined with a unique GID.
Legacy ID: SV-107081
Legacy ID: V-97977

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 an ACF Command screen enter:
SET PROFILE(GROUP) DIVISION(OMVS)
LIST LIKE(-)

If each of the definitions have a unique GID, this is not a finding.

Fix Text: Define each UNIX group with a unique GID.

CCI: CCI-000764

Group ID (Vulid): V-223637
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223637r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000220
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-107083
Legacy ID: V-97979

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:

ACF
SET PROFILE(GROUP) DIVISION(OMVS)
LIST LIKE(-)

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-223638
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223638r858918_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-US-000230
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-107085
Legacy ID: V-97981

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 this is a Classified system, this is Not Applicable.

From an ACF2 command line enter:
SET CONTROL(GSO)
SHOW UNIXOPTS

Alternately:
Refer to the following report produced by the ACF2 Data Collection:
- ACF2CMDS.RPT(ACFGSO)
- ACF2CMDS.RPT(OMVSUSER)

Note: This check applies to any user identifier (LOGONID) used to model OMVS access on the mainframe. This includes any DFTUSER; MODLUSER and BPX.UNIQUE.USER. If MODLUSER is specified then UNIQUSER must be specified.

If DFTUSER or MODLUSER is not defined in the UNIXOPTS record, this is not a finding.

If ALL user identifiers (LOGONID) defined to DFTUSER or MODLUSER. or BPX.UNIQUE.USER user account is defined as follows, this is not a 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: Define DFTUSER or MODLUSER or BPX.UNIQUE.USER user account to be defined as follows:

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).

Example:
SET PROFILE(USER) DIV(OMVS)
LIST OMVS

INSERT OMVS HOME(/) OMVSPGM(/bin/false) UID(0)

CCI: CCI-000764

Group ID (Vulid): V-223639
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223639r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-UT-000010
Rule Title: IBM z/OS startup user account for the z/OS UNIX Telnet Server must be defined properly.
Legacy ID: SV-107087
Legacy ID: V-97983

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
ls (to make sure OTELNET is active)
cat otelnetd.conf

If the otelnetd command specifies OMVS or OMVSKERN as the user, this is not a finding.

If the otelnetd command specifies any user other than OMVS or OMVSKERN, this is a finding.

Fix Text: Configure the otelnetd startup command in the inetd.conf file to be defined for the z/OS UNIX kernel.

CCI: CCI-000213

Group ID (Vulid): V-223640
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223640r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-UT-000020
Rule Title: IBM z/OS HFS objects for the z/OS UNIX Telnet Server must be properly protected.
Legacy ID: SV-107089
Legacy ID: V-97985

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-223641
Group Title: SRG-OS-000024-GPOS-00007
Rule ID: SV-223641r560914_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-UT-000030
Rule Title: IBM z/OS UNIX Telnet Server etc/banner file must have the Standard Mandatory DoD Notice and Consent Banner.
Legacy ID: V-97987
Legacy ID: SV-107091

Vulnerability Discussion: A logon banner can be used to inform users about the environment during the initial logon. In the DISA environment, logon banners are used to warn users against unauthorized entry and the possibility of legal action for unauthorized users, and advise all users that system use constitutes consent to monitoring. Failure to display a logon warning banner without this type of information could adversely impact the ability to prosecute unauthorized users and users who abuse the system.

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: Preferably 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 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.

CCI: CCI-000048

CCI: CCI-000050

Group ID (Vulid): V-223642
Group Title: SRG-OS-000228-GPOS-00088
Rule ID: SV-223642r864508_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-UT-000040
Rule Title: IBM z/OS UNIX Telnet Server warning banner must be properly specified.
Legacy ID: V-97989
Legacy ID: SV-107093

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.

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-223643
Group Title: SRG-OS-000228-GPOS-00088
Rule ID: SV-223643r864509_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-UT-000050
Rule Title: IBM z/OS UNIX Telnet Server Startup parameters must be properly specified to display the banner.
Legacy ID: V-97991
Legacy ID: SV-107095

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.

Check Content:
From the ISPF Command Shell enter:

OMVS
CD /etc
cat inetd.config

If "-h" is included on the otelnetd statement, this is a finding. ("-h" indicates that a banner will not be displayed.)

Fix Text: Configure the otelnetd startup command in the inetd.conf file to not include "-h".

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

Group ID (Vulid): V-223644
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223644r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-VT-000010
Rule Title: IBM z/OS System data sets used to support the VTAM network must be properly secured.
Legacy ID: V-97993
Legacy ID: SV-107097

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.

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.

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 ACF2 data set rules for all VTAM system data sets do not restrict access to only network systems programming staff, this is a finding.
If ACF2 data set rules for all VTAM system data sets do not restrict auditors to READ access only, this is a finding.

These data sets include libraries containing VTAM load modules and exit routines, and VTAM start options and definition statements.

Fix Text: Define ACF2 data set rules for all VTAM system data sets to restrict access to only network systems programming staff.
Auditors may have READ access as documented and approved by ISSM.

These data sets include libraries containing VTAM load modules and exit routines, and VTAM start options and definition statements.

Example:
$KEY(SYS1)
VTAM-.- UID(sysprgmr) R(A) W(L) A(L) E(A)

$KEY(S3V)
$PREFIX(SYS3)
VTAM-.- UID(sysprgmr) R(A) W(L) A(L) E(A)

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-223645
Group Title: SRG-OS-000259-GPOS-00100
Rule ID: SV-223645r533198_rule
Severity: CAT II
Rule Version (STIG-ID): ACF2-VT-000020
Rule Title: IBM z/OS VTAM USSTAB definitions must not be used for unsecured terminals.
Legacy ID: V-97995
Legacy ID: SV-107099

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 must 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
