

UNCLASSIFIED



IBM z/OS RACF Security Technical Implementation Guide

Version: 8

Release: 12

26 Jul 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-223646

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-223646r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-CE-000010](#)

Rule Title: Certificate Name Filtering must be implemented with appropriate authorization and documentation.

Legacy ID: V-97997

Legacy ID: SV-107101

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:

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

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:

Currently the RACDCERT command does not support a generic userid value of ID(*) LISTMAP to list all the certificate name filters defined to RACF. However, the following commands can be issued to determine if certificate name filtering may be implemented.

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 SETROPTS LIST command. If the DIGTNMAP resource class is active, RACF is ready to process any certificate name filters with a Status of TRUST. The DIGTNMAP resource class should not be active unless certificate name filtering is desired.

If the DIGTNMAP resource class is not active, this is not a finding.

Certificate name filters are stored as profiles in the DIGTNMAP resource class. The RLIST

command is not intended for use with profiles in the DIGTNMAP resource class. However it can be used to determine if any profiles are defined. (NOTE: The information will not be displayed in a suitable format to easily interpret the filter.)

RLIST DIGTNMAP *

If there is nothing to list in the DIGTNMAP resource class, this is not a finding.

If profile information is displayed, one or more certificate name filters are defined to RACF. Under the NAME heading of each profile listing is the userid the filter is being mapped to. Issue the following command the list the certificate name filter associated with each userid:

RACDCERT ID(profile name userid) LISTMAP

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

If the DIGTNMAP resource class is active 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: Ensure any certificate name filtering rules in use are documented and approved by the ISSM.

CCI: CCI-000764

Group ID (Vulid): V-223647

Group Title: SRG-OS-000066-GPOS-00034

Rule ID: SV-223647r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-CE-000020](#)

Rule Title: Expired digital certificates must not be used.

Legacy ID: V-97999

Legacy ID: SV-107103

Vulnerability Discussion: The longer and more often a key is used, the more susceptible it is to loss or discovery. This weakens the assurance provided to a relying Party that the unique binding between a key and its named subscriber is valid. Therefore, it is important that certificates are

periodically refreshed. This is in accordance with DoD requirement. Expired Certificate must not be in use.

Check Content:

From the ISPF Command Shell enter:
RACDCERT CERTAUTH LIST

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.

Check the expiration (End Date) for each certificate with a status of TRUST.

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

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

CCI: CCI-000185

Group ID (Vulid): V-223648

Group Title: SRG-OS-000066-GPOS-00034

Rule ID: SV-223648r868789_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-CE-000030](#)

Rule Title: All digital certificates in use must have a valid path to a trusted Certification authority.

Legacy ID: V-98001

Legacy ID: SV-107105

Vulnerability Discussion: The origin of a certificate, the Certificate Authority (i.e., CA), is crucial in determining if the certificate should be trusted. An approved CA establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

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

Check Content:

From the ISPF Command Shell enter:

RACDCERT CERT AUTH

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 maybe 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 and/or replace certificates with a status of TRUST whose 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.

Reference the DoD Cyber Exchange website for complete information as to which certificates may be acceptable (<https://public.cyber.mil/pki-pke/interoperability/> or <https://cyber.mil/pki-pke/interoperability/>).

CCI: CCI-000185

CCI: CCI-002470

Group ID (Vulid): V-223649

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223649r853567_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000010](#)

Rule Title: IBM RACF must limit Write or greater access to SYS1.NUCLEUS to system programmers only.

Legacy ID: V-98003

Legacy ID: SV-107107

Vulnerability Discussion: This data set contains a large portion of the system initialization (IPL) programs and pointers to the master and alternate master catalog. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

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

Check Content:

Execute a dataset access list for SYS1.NUCLEUS.

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

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

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

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223650

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223650r853568_rule

Severity: CAT III

Rule Version (STIG-ID): [RACF-ES-000020](#)

Rule Title: IBM RACF must limit Write or greater access to libraries that contain PPT modules to system programmers only.

Legacy ID: V-98005

Legacy ID: SV-107109

Vulnerability Discussion: Specific PPT designated program modules possess significant security bypass capabilities. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

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

Check Content:

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

```
TSO ISRDDN LOAD IEFSDPPT
```

Press Enter.

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

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

- The ACP data set rules for libraries that contain PPT modules do not restrict WRITE or greater access to only z/OS systems programming personnel.

- The ACP data set rules for libraries that contain PPT modules do not specify that all WRITE or greater access will be logged.

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

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-235033

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-235033r853641_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000030](#)

Rule Title: IBM RACF must limit WRITE or greater access to LINKLIST libraries to system programmers only.

Legacy ID: SV-107111

Legacy ID: V-98007

Vulnerability Discussion: The primary function of the LINKLIST is to serve as a single repository for commonly used system modules. Failure to ensure that the proper set of libraries is designated for LINKLIST can impact system integrity, performance, and functionality. For this reason, controls must be employed to ensure that the correct set of LINKLIST libraries is used. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

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

Check Content:

From Any ISPF input line, enter:
TSO ISRDDN LINKLIST

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

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

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

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

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

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

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223652

Group Title: SRG-OS-000123-GPOS-00064

Rule ID: SV-223652r803635_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000040](#)

Rule Title: IBM RACF emergency USERIDs must be properly defined.

Legacy ID: SV-107113

Legacy ID: V-98009

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 a list of all emergency userids available to the site along with the associated function of each userid.

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.

Execute an access list for each emergency userid.

If emergency userids exist at a minimum an emergency logonid will exist with the security administration attributes specified in accordance with the following requirements.

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

At least one userid exists to perform RACF security administration. These userids are defined to

RACF with the system-SPECIAL attribute. They must not have the OPERATIONS attribute.

If any userids exist to perform operating system functions, they are defined without any RACF security administration privileges. These userids are defined to RACF with the system-OPERATIONS attribute, and FULL access to all DASD volumes. They must not have the SPECIAL attribute.

NOTE: A user who has the system-OPERATIONS attribute has FULL access authorization to all RACF-protected resources in the DASDVOL/GDASDVOL resource classes. However, if their userid or any associated group (i.e., default or connect) is in the access list of a resource profile, they will only have the access specified in the access list.

All emergency userids are defined to RACF and SYS1.UADS.

All emergency logonid/logonid(s) are to be implemented with logging to provide an audit trail of their activities. This is accomplished with the UAUDIT attribute.

All emergency logonid/logonid(s) will have distinct, different passwords in SYS1.UADS and in RACF, 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 RACF.

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.

Fix Text: Configure emergency USERIDs to have access granted only authorizes those resources required to support the specific functions of either DASD Recovery or System Administration.

Ensure the following items are in effect regarding emergency userids:

At a minimum an emergency userids will exists with the security administration attributes specified in accordance with the following requirements:

- Userids exist to perform RACF security administration only. These userids are defined to RACF with the system-SPECIAL attribute. They must not have the OPERATIONS attribute. Emergency userids will have either SPECIAL or OPERATIONS but not both.

- Userids can be defined to perform operating system functions. Such userids must be defined without any RACF security administration privileges. These userids are defined to RACF with the system-OPERATIONS attribute, FULL access to all DASD volumes resources as well as the FACILITY Class STGADMN profiles. They must not have the SPECIAL attribute.

NOTE: A user who has the system-OPERATIONS attribute has FULL access authorization to all RACF-protected resources in the DASDVOL/GDASDVOL resource classes. However, if their

userid or any associated group (i.e., default or connect) is in the access list of a resource profile, they will only have the access specified in the access list since access lists override OPERATIONS.

- Userids exist to perform RACF security administration only. These userids are defined to RACF with the system-SPECIAL attribute. They must not have the OPERATIONS attribute. Emergency userids will have either SPECIAL or OPERATIONS but not both.

- All emergency userids are defined to RACF and SYS1.UADS. See TSO Command Ref for info on adding users to UADS.

- All emergency userids are to be implemented with logging to provide an audit trail of their activities. This is accomplished with the UAUDIT attribute via the command:

```
ALU <uid> UAUDIT
```

- All emergency userids will have distinct, different passwords in SYS1.UADS and in RACF, 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 RACF.

- All emergency userids will have documented procedures - such as a COOP Plan - 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 userids is released for use, its password is to be reset by the ISSO within 12 hours.

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

CCI: CCI-001682

Group ID (Vulid): V-223653

Group Title: SRG-OS-000004-GPOS-00004

Rule ID: SV-223653r868792_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000050](#)

Rule Title: IBM RACF SETROPTS LOGOPTIONS must be properly configured.

Legacy ID: SV-107115

Legacy ID: V-98011

Vulnerability Discussion: Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to create an account. Auditing account creation actions provides logging that can be used for forensic purposes.

To address access requirements, many operating systems may be integrated with enterprise level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-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-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, 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-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:

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

Verify that the following LOGOPTIONS are specified:

LOGOPTIONS "FAILURES" CLASSES = <all the classes listed in the "ACTIVE" class as a minimum>

LOGOPTIONS "NEVER" CLASSES = NONE

The other LOGOPTIONS may be site determined.

If the LOGOPTIONS are not set as described above, 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 in the example below:

Ensure that the following LOGOPTIONS are specified:

LOGOPTIONS "FAILURES" CLASSES = <all the classes listed in the "ACTIVE" class as a minimum>

LOGOPTIONS "NEVER" CLASSES = NONE

The other LOGOPTIONS may be site determined.

CCI: CCI-000018

CCI: CCI-000131

CCI: CCI-000132

CCI: CCI-000133

CCI: CCI-000134

CCI: CCI-000135

CCI: CCI-000172

CCI: CCI-001404

CCI: CCI-001405

CCI: CCI-002884

Group ID (Vulid): V-223654

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223654r868794_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000060](#)

Rule Title: IBM RACF must protect memory and privileged program dumps in accordance with proper security requirements.

Legacy ID: SV-107117

Legacy ID: V-98013

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:

Execute a resource access list for the IEAABD. resources.

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

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

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

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

Fix Text: Memory and privileged program dump resources are provided via resources in the FACILITY resource class. Configure these resources to the ESM as specified in the following.

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

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

IEAABD.
IEAABD.DMPAUTH.
IEAABD.DMPAKEY.

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

Ensure that no access is given to "IEAABD." resource.

Example:

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

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

Example:

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

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

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

Example:

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

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

CCI: CCI-000213

Group ID (Vulid): V-223655

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223655r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000070](#)

Rule Title: IBM z/OS system commands must be properly protected.

Legacy ID: V-98015

Legacy ID: SV-107119

Vulnerability Discussion: z/OS system commands provide a method of controlling the operating environment. Failure to properly control access to z/OS system commands could result in unauthorized personnel issuing sensitive system commands. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Check Content:

From the ISPF Command Shell enter:

```
RList OPERCMDS *
```

If the MVS.** resource is defined to the OPERCMDS class with an access of NONE and all (i.e., failures and successes) access logged, this is not a finding.

If the 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.

If all access (i.e., failures and successes) to specific z/OS system commands is logged as indicated in the table entitled MVS commands, RACF access authorities, and resource names, in the z/OS MVS System Commands, this is not a finding.

Fix Text: z/OS system commands provide control over z/OS functions and can compromise security if misused. These commands are subject to various types of potential abuse. For this reason, it is necessary to place restrictions on the z/OS system commands that can be entered by particular operators.

Some commands are particularly dangerous and should only be used when all less drastic options have been exhausted. Misuse of these commands can create a situation in which the only recovery is an IPL.

Apply the following recommendations when implementing security:

The MVS.** resource is defined to the OPERCMDS class with an access of NONE and all (i.e., failures and successes) access logged.

Access to z/OS system commands defined in the 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).

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

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.

All elevated access (i.e., failures and successes) to specific z/OS system commands is logged.

A sample set of commands to define and permit access to system command resources is shown here:

```
RDEF OPERCMDS MVS.** UACC(NONE) OWNER(<syspsmpl>) AUDIT(ALL(READ))  
DATA("set up deny-by-default profile')
```

Then, in accordance with the referenced table, use the following template to define profiles for each command:

```
RDEF OPERCMDS <system command profile> UACC(NONE) OWNER(<syspsmpl>)  
AUDIT(ALL(READ))
```

```
PERMIT <system command profile> CLASS(OPERCMDS) ID(<groupname>)
```


ACCESS(<accesslevel>)

CCI: CCI-000213

Group ID (Vulid): V-223656

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223656r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000080](#)

Rule Title: IBM RACF must properly define users that have access to the CONSOLE resource in the TSOAUTH resource class.

Legacy ID: V-98017

Legacy ID: SV-107121

Vulnerability Discussion: 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:

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

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

If Userids are restricted to the INFO level on the AUTH parameter specified in the OPERPARM segment of their userid, this is not a finding.

If Userids are restricted to READ access to the MVS.MCSOPER.userid resource defined in the OPERCMDS resource class, this is not a finding.

If Userids and/or group IDs are restricted to READ access to the CONSOLE resource defined in the TSOAUTH resource class, this is not a finding.

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

Ensure the following items are in effect for all MCS consoles:

Define a profile protecting the use of the CONSOLE command within TSO. A sample command to accomplish this is shown here: RDEF TSOAUTH CONSOLE UACC(NONE)
OWNER(ADMIN) AUDIT(ALL(READ))

Permit only authorized users. A sample command to accomplish this is shown here: PE
CONSOLE CL(TSOAUTH) ID(<syspsmpl>)

Set up the OPERPARM segment in corresponding user-class entry. A sample command to
accomplish this is shown here: ALU <authorized user> OPERPARM(AUTH(INFO))

Userids are restricted to READ access to the MVS.MCSOPER.userid resource defined in the
OPERCMDSD resource class. A sample command to accomplish this is shown here using the
GLOBAL class:

```
RDEF GLOBAL OPERCMDSD ADDMEM(MVS.MCSOPER.&RACUID/READ)  
OWNER(ADMIN)
```

CCI: CCI-000213

Group ID (Vulid): V-223657

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223657r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000090](#)

Rule Title: The IBM RACF FACILITY resource class must be active.

Legacy ID: V-98019

Legacy ID: SV-107123

Vulnerability Discussion: IBM Provides the FACILITY Class for use in protecting a variety of
features/functions/products both IBM and third-party. The FACILITY Class is not dedicated to
any one specific use and is intended as a multi-purpose RACF Class. Failure to activate this class
will result in unprotected resources. This exposure may threaten the integrity of the operating
system environment, and compromise the confidentiality of customer data.

Check Content:

The RACF Command SETR LIST will show the status of RACF Controls including a list of
ACTIVE classes.

From the ISPF Command Shell enter:

SETRopts List

If the FACILITY resource class is active, this is not a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a
plan of action to implement the control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including a list of ACTIVE classes.

The FACILITY Class is activated with the command SETR CLASSACT(FACILITY).

Generic profiles and commands should also be enabled with the command SETR GENERIC(FACILITY) GENCMD(FACILITY).

IBM recommends RACLISTing the FACILITY Class which is accomplished with the command SETR RACL(FACILITY).

CCI: CCI-000213

Group ID (Vulid): V-223658

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223658r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000100](#)

Rule Title: The IBM RACF OPERCMDS resource class must be active.

Legacy ID: V-98021

Legacy ID: SV-107125

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:

The RACF Command SETR LIST will show the status of RACF Controls including a list of ACTIVE classes.

From the ISPF Command Shell enter:

SETRopts List

If the OPERCMDS resource class is active, this is not a finding.

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

plan of action to implement the control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including a list of ACTIVE classes.

The OPERCMDS Class is activated with the command SETR CLASSACT(OPERCMDS).

Generic profiles and commands should also be enabled with the command SETR GENERIC(OPERCMDS) GENCMD(OPERCMDS).

IBM recommends RACLISTing the OPERCMDSClass which is accomplished with the command SETR RACL(OPERCMDS).

CCI: CCI-000213

Group ID (Vulid): V-223659

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223659r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000110](#)

Rule Title: The IBM RACF MCS consoles resource class must be active.

Legacy ID: V-98023

Legacy ID: SV-107127

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:

The RACF Command SETR LIST will show the status of RACF Controls including a list of ACTIVE classes.

From the ISPF Command Shell enter:
SETRopts List

If the CONSOLE resource class is active, this is not a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including a list of ACTIVE classes.

The CONSOLE Class is activated with the command SETR CLASSACT(CONSOLE).

Generic profiles and commands should also be enabled with the command SETR GENERIC(CONSOLE) GENCMD(CONSOLE).

IBM recommends RACLISTing the CONSOLE Class which is accomplished with the command SETR RACL(CONSOLE).

CCI: CCI-000213

Group ID (Vulid): V-223660

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223660r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000120](#)

Rule Title: IBM RACF CLASSACT SETROPTS must be specified for the TEMPDSN class.

Legacy ID: V-98025

Legacy ID: SV-107129

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:

The RACF Command SETR LIST will show the status of RACF Controls including a list of ACTIVE classes.

From the ISPF Command Shell enter:
SETRopts List

If the TEMPDSN resource class is ACTIVE, this is not a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including a list of ACTIVE classes.

The TEMPDSN Class is activated with the command SETR CLASSACT(TEMPDSN).

Generic profiles and commands should also be enabled with the command SETR GENERIC(TEMPDSN) GENCMD(TEMPDSN).

IBM recommends RACLISTing the TEMPDSN Class which is accomplished with the command SETR RACL(TEMPDSN).

CCI: CCI-000213

Group ID (Vulid): V-223661

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223661r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000130](#)

Rule Title: IBM RACF started tasks defined with the trusted attribute must be justified.

Legacy ID: V-98027

Legacy ID: SV-107131

Vulnerability Discussion: Trusted Started tasks bypass RACF checking. It is vital that this attribute is NOT granted to unauthorized Started Tasks which could then obtain unauthorized access to the system. This could result in the compromise of the confidentiality, integrity, and availability of the operating system, ACP, or customer data.

Check Content:

Refer to the list of z/OS started tasks and address spaces in the IBM z/OS MVS Initialization and Tuning Reference.

If the only approved Started Tasks that have the TRUSTED flag enabled are in this list, this is not a finding.

If there are no Started Tasks that have been granted the PRIVILEGED attribute, this is not a finding.

Guidelines for reference:

Assign the TRUSTED attribute when one of the following conditions applies:

- The started procedure or address space creates or accesses a wide variety of unpredictably named data sets within your installation.
- Insufficient authority to an accessed resource might risk an unsuccessful IPL or other system problem.

Avoid assigning TRUSTED to a z/OS started procedure or address space unless it is listed here or you are instructed to do so by the product documentation.

Additionally external security managers are candidates for trusted attribute.

Any other started tasks not listed or not covered by the guidelines are a finding unless approval by the Authorizing Official.

Fix Text: Review assignment of the TRUSTED attribute in ICHRIN03 and/or the STARTED resource class. Ensure only those trusted STCs that are listed in the IBM z/OS MVS Initialization and Tuning Reference have been granted this authority. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes. 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.

The TRUSTED attribute can be removed from a STARTED class profile using the command:
RALT STARTED <profilename> STDATA(TRUSTED(NO))

If the STARTED class is RACLISTed then a refresh command is necessary:
SETR RACL(STARTED) REFRESH

If any Started Tasks exist with the PRIVILEGED attribute then take the following action to remove this attribute:
RALT STARTED <profilename> STDATA(PRIVILEGED(NO))

If the STARTED class is RACLISTed then a refresh command is necessary:

SETR RACL(STARTED) REFRESH

CCI: CCI-000213

Group ID (Vulid): V-223662

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223662r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000140](#)

Rule Title: IBM RACF USERIDs possessing the Tape Bypass Label Processing (BLP) privilege must be justified.

Legacy ID: V-98029

Legacy ID: SV-107133

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:

```
RLIST FACILITY ICHBLP AUTHUSER
```

If access authorization to the ICHBLP resource is restricted at the userid level to data center personnel (e.g., tape librarian, operations staff, etc.), this is not a finding.

If no tape management system (e.g., CA-1) is installed the following:

From the ISPF Command Shell enter:

```
SETROPTS LIST
```

If the TAPEVOL class is active, this is not a finding.

Fix Text: Review all USERIDs with the BLP attribute. Ensure documentation providing justification for access is maintained and filed with the ISSO, and that unjustified access is removed.

BLP is controlled thru the FACILITY class profile ICHBLP. Access is removed with the

following command:

```
PE ICHBLP CL(FACILITY) id(<userid>) DELETE
```

a subsequent REFRESH of the FACILITY class may be required via the command: SETR
RACL(FACILITY) REFRESH

CCI: CCI-000213

Group ID (Vulid): V-223663

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223663r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000150](#)

Rule Title: IBM RACF DASD volume-level protection must be properly defined.

Legacy ID: SV-107135

Legacy ID: V-98031

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:

```
RLIST DASDVOL AUTHUSER
```

If a profile of "***" is defined for the "DASDVOL" resource class, this is not finding.

If access authorization to "DASDVOL" profiles is restricted to Storage Management Personnel, Storage Management Batch Userids, and Systems Programmers, this is not a finding.

If all (i.e., failures and successes) access is logged, this is not a finding.

Fix Text: Develop a plan of action to implement the required changed.

Define profiles in the "DASDVOL" class. A sample command is provided here:

```
RDEF DASDVOL ** UACC(NONE) OWNER(<StgMgmtGrp>) AUDIT(ALL(READ)).
```

More specific "DASDVOL" profiles should be defined to protect groups of "DASDVOLs". A sample command to create a profile protecting all DASDVOLs beginning with "SYS" is provided here:

```
RDEF DASDVOL SYS* UACC(NONE) OWNER(<StgMgmtGrp>) AUDIT(ALL(READ)).
```

Permission can be granted to "DASDVOL" profiles. A sample command is provided here:
PE SYS* CLASS(DASDVOL) ID(<syspsmpl>) ACCESS(ALTER)

If any profiles are in "WARN" mode, they should be reset. A sample command is provided here:
RALT DASDVOL <profilename> NOWARN.

Note that the "GDASDVOL" class can also be used. See the RACF Security Admin Guide for more information.

CCI: CCI-000213

Group ID (Vulid): V-223664

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223664r868797_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000160](#)

Rule Title: IBM Sensitive Utility Controls must be properly defined and protected.

Legacy ID: SV-107137

Legacy ID: V-98033

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

Check Content:

If the RACF resource access authorizations for the following sensitive utilities restrict access to the appropriate personnel according to the site security plan, this is not a finding.

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

Ensure that all Sensitive Utility Controls resources and/or generic equivalent are properly protected according to the site security plan.

Use Sensitive Utility Controls table below that lists the resources, access requirements, and logging requirements for Sensitive Utilities, ensuring the following guidelines are followed:

Sensitive Utility Controls

Program Product Function

AHLGTF z/OS System Activity Tracing

HHLGTF

IHLGTF

ICPIOCP z/OS System Configuration

IOPIOCP

IXPIOCP

IYPIOCP

IZPIOCP

BLSROPTR z/OS Data Management

DEBE OS/DEBE Data Management

DITTO OS/DITTO Data Management

FDRZAPOP FDR Product Internal Modification

GIMSMP SMP/E Change Management Product

ICKDSF z/OS DASD Management

IDCSC01 z/OS IDCAMS Set Cache Module

IEHINITT z/OS Tape Management

IFASMFDP z/OS SMF Data Dump Utility

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

CSQJU003 IBM WebSphereMQ

CSQJU004

CSQUCVX

CSQ1LOGP

CSQUTIL

WHOIS z/OS Share MOD to identify user name from USERID.

Restricted to data center personnel only.

The RACF resources as designated in the table above are defined with a default access of NONE.

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

The RACF resource rules for the resources designated in the table above specify UACC(NONE) and NOWARNING.

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

```
RDEF PROGRAM AHLGTF ADDMEM('SYS1.LINKLIB'//NOPADCHK) -  
DATA('ADDED PER SRR PDI RACF0770 ') -  
AUDIT(ALL(READ)) UACC(NONE) OWNER(ADMIN)  
PERMIT AHLGTF CLASS(PROGRAM) ID(stcgsmpl)
```

CCI: CCI-000213

Group ID (Vulid): V-223665

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223665r868800_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000170](#)

Rule Title: IBM RACF Global Access Checking must be restricted to appropriate classes and resources.

Legacy ID: SV-107139

Legacy ID: V-98035

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 a command input screen enter:

RL Global *

If Global * is specified in SETROPTS, this is a finding.

The following entries may be allowed with the approval of the ISSM:

Dataset Class - ALTER access level to &RACUID.** (Allows users all access to their own datasets)

OPERCMDS Class - READ access to MVS.MCSOPER.&RACUID (Allows users access to console for their jobs)

JESJOBS Class - ALTER access to CANCEL.*.*&RACUID (Allows users to cancel their own jobs)

JESJOBS Class - ALTER access to SUBMIT.*.*&RACUID (Allows users to submit their own jobs)

The ISSM may allow other classes to be included after evaluation with the system programmer.

If any other members are included for Global Access Checking, this is a finding.

If written approval by the ISSM is not provided, this is a finding.

Fix Text: Configure Global Access Checking to be appropriately administered.

Evaluate the impact associated with implementation of the control option. Develop approval documentation and a plan of action to implement the control option as specified in the example below:

RALT GLOBAL class-name

ADDMEM (resourcename)/accesslevel)

CCI: CCI-000213

Group ID (Vulid): V-223666

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223666r868803_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000180](#)

Rule Title: IBM RACF access to the System Master Catalog must be properly protected.

Legacy ID: SV-107141

Legacy ID: V-98037

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

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

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

Check Content:

Refer to SYSCATxx member of SYS1.NUCLEUS.

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

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

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

If Products or procedures requiring system programmer access for system-level maintenance meet the following specific case, this is not a finding:

- The batch job or procedure must be documented in the SITE Security Plan.
- Reside in a data set that is restricted to systems programmers' access only.

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

Fix Text: Review access authorization to critical system files.

Evaluate the impact of correcting the deficiency.

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

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

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

Configure ESM rules for the master catalog to allow any products or procedures system programmer access for system-level maintenance that 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.

All greater than read access must be logged.

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223667

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223667r853573_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000190](#)

Rule Title: IBM RACF must limit Write or greater access to SYS1.UADS to system programmers only, and WRITE or greater access must be limited to system programmer personnel and/or security personnel.

Legacy ID: V-98039

Legacy ID: SV-107143

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

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

Check Content:

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

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

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

The ESM data set rules for SYS1.UADS specify that all (i.e., failures and successes) data set access authorities (i.e., READ, UPDATE, ALTER, 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 UPDATE access should be limited to the security staff.

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

Configure allocate access to SYS1.UADS to be limited to system programmers only, Read and Update access to SYS1.UADS to be limited to system programmer personnel and/or security personnel, and all dataset access is logged.

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223668

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223668r868805_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000200](#)

Rule Title: IBM z/OS must protect dynamic lists in accordance with proper security requirements.

Legacy ID: V-98041

Legacy ID: SV-107145

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 RACF command:

RLIST FACILITY *

If the RACF resources and/or generic equivalent identified below are defined with AUDIT(ALL(READ)) and WRITE or greater 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 RACF CSVDYNEX.LIST resource and/or generic equivalent is defined with AUDIT(FAILURE(READ)SUCCESS(UPDATE)) and WRITE or greater access restricted to system programming personnel, this is not a finding.

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

If the products CICS and/or CONTROL-O are on the system, the RACF access to the CSVLLA resource and/or generic equivalent will be defined with AUDIT(ALL) and UPDATE access restricted to the CICS and CONTROL-O STC userids.

If any software product requires access to dynamic LPA updates on the system, the RACF 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.

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

Fix Text: Configure the Dynamic List resources to be defined to the RACF FACILITY resource class and protected. Only system programmers and a limited number of authorized users and approved authorized Started Tasks are able to issue these commands. All access is logged.

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

CSVAPF.**
CSVAPF.MVS.SETPROG.FORMAT.DYNAMIC

CSVAPF.MVS.SETPROG.FORMAT.STATIC
CSVDYLPA.**
CSVDYLPA.ADD.**
CSVDYLPA.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 AUDIT(ALL(READ)) and UPDATE access.

Sample commands are shown here to accomplish this:

```
RDEF FACILITY CSVAPF.** UACC(NONE) OWNER(syspsmpl) AUDIT(ALL(READ))
RDEF FACILITY CSVAPF.MVS.SETPROG.FORMAT.DYNAMIC.** UACC(NONE)
OWNER(syspsmpl) AUDIT(ALL(READ))
RDEF FACILITY CSVAPF.MVS.SETPROG.FORMAT.STATIC.** UACC(NONE)
OWNER(syspsmpl) AUDIT(ALL(READ))
```

```
PERMIT CSVAPF.** CLASS(FACILITY) ID(syspsmpl) ACCESS(UPDATE)
PERMIT CSVAPF.MVS.SETPROG.SETPROG.FORMAT.DYNAMIC.** CLASS(FACILITY)
ID(syspsmpl) ACCESS(UPDATE)
PERMIT CSVAPF.MVS.SETPROG.SETPROG.FORMAT.STATIC.** CLASS(FACILITY)
ID(syspsmpl) ACCESS(UPDATE)
```

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

The CSVDYLPA.DELETE resource will be permitted to products CA 1 and CA Common Services STC userids with AUDIT(ALL(READ)) and UPDATE access.

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

```
RDEF FACILITY CSVDYLPA.** UACC(NONE) OWNER(syspsmpl) AUDIT(ALL(READ))
RDEF FACILITY CSVDYLPA.ADD.** UACC(NONE) OWNER(syspsmpl)
AUDIT(ALL(READ))
RDEF FACILITY CSVDYLPA.DELETE.** UACC(NONE) OWNER(syspsmpl)
AUDIT(ALL(READ))
```

```
PERMIT CSVDYLPA.** CLASS(FACILITY) ID(syspsmpl) ACCESS(UPDATE)
PERMIT CSVDYLPA.** CLASS(FACILITY) ID(BMC Mainview STC userid)
ACCESS(UPDATE)
PERMIT CSVDYLPA.** CLASS(FACILITY) ID(CA 1 STC userid) ACCESS(UPDATE)
PERMIT CSVDYLPA.** CLASS(FACILITY) ID(CCS STC userid) ACCESS(UPDATE)
```

```
PERMIT CSVDYLPA.ADD.** CLASS(FACILITY) ID(syspsmpl) ACCESS(UPDATE)
PERMIT CSVDYLPA.ADD.** CLASS(FACILITY) ID(BMC Mainview STC userid)
ACCESS(UPDATE)
PERMIT CSVDYLPA.ADD.** CLASS(FACILITY) ID(CA 1 STC userid) ACCESS(UPDATE)
PERMIT CSVDYLPA.ADD.** CLASS(FACILITY) ID(CCS STC userid) ACCESS(UPDATE)
PERMIT CSVDYLPA.DELETE.** CLASS(FACILITY) ID(syspsmpl) ACCESS(UPDATE)
PERMIT CSVDYLPA.DELETE.** CLASS(FACILITY) ID(CA 1 STC userid)
ACCESS(UPDATE)
PERMIT CSVDYLPA.DELETE.** CLASS(FACILITY) ID(CCS STC userid)
ACCESS(UPDATE)
```

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

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

Sample commands are shown here to accomplish this:

```
RDEF FACILITY CSVDYNEX.** UACC(NONE) OWNER(syspsmpl) -
AUDIT(ALL(READ))
RDEF FACILITY CSVDYNEX.LIST.** UACC(NONE) OWNER(syspsmpl) -
AUDIT(FAILURE(READ)SUCCESS(UPDATE))
```

```
PERMIT CSVDYNEX.** CLASS(FACILITY) ID(syspsmpl) ACCESS(UPDATE)
PERMIT CSVDYNEX.LIST.** CLASS(FACILITY) ID(syspsmpl) ACCESS(UPDATE)
PERMIT CSVDYNEX.LIST.** CLASS(FACILITY) ID(smplsmpl) ACCESS(READ)
```

The CSVLLA resource will be permitted to CICS and CONTROL-O STC userids with AUDIT(ALL(READ)) and UPDATE access.

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

```
RDEF FACILITY CSVLLA.** UACC(NONE) OWNER(syspsmpl) AUDIT(ALL(READ))

PERMIT CSVLLA.** CLASS(FACILITY) ID(syspsmpl) ACCESS(UPDATE)
PERMIT CSVLLA.** CLASS(FACILITY) ID(CICS STC userids) ACCESS(UPDATE)
PERMIT CSVLLA.** CLASS(FACILITY) ID(CONTROL-O STC userid)
ACCESS(UPDATE)
```

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223669

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223669r868808_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000210](#)

Rule Title: IBM RACF allocate access to system user catalogs must be properly protected.

Legacy ID: V-98043

Legacy ID: SV-107147

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:

From the ISPF Command Shell enter:

```
LISTCat USERCATALOG ALL NOPREFIX
```

Review the ESM data set rules for each usercatalog defined.

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

If Products or procedures requiring system programmer access for system-level maintenance meets the following specific case, this is not a finding:

- The batch job or procedure must be documented in the SITE Security Plan.
- Reside in a data set that is restricted to systems programmers' access only.

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

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

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

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

Configure ESM rules for the USER CATALOGS to allow any products or procedures system programmer access for system-level maintenance that 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 data sets UPDATE access is required for user operation.

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223670

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223670r853576_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000220](#)

Rule Title: IBM RACF must limit WRITE or greater access to System backup files to system programmers and/or batch jobs that perform DASD backups.

Legacy ID: V-98045

Legacy ID: SV-107149

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:

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

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

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

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

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223671

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223671r853577_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000230](#)

Rule Title: IBM RACF must limit access to SYS(x).TRACE to system programmers only.

Legacy ID: V-98047

Legacy ID: SV-107151

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 dataset list of access for SYS(x).TRACE files.

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

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

Fix Text: Configure the ESM access to SYS1.TRACE to be limited to system programmers or started tasks that perform GTF processing.

Other user access can be granted as documented and approved by the ISSM.

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223672

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223672r853578_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000240](#)

Rule Title: IBM RACF batch jobs must be properly secured.

Legacy ID: V-98049

Legacy ID: SV-107153

Vulnerability Discussion: Batch jobs that are submitted to the operating system should inherit the USERID of the submitter. This will identify the batch job with a userid for the purpose of accessing resources. BATCHALLRACF ensures that a valid USERID is associated with batch jobs. Jobs that are submitted to the operating system via a scheduling facility must also be identified to the system. Without a batch job having an associated USERID, access to system resources will be limited.

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000326-GPOS-00126

Check Content:

Refer to the documentation of the processes used for submission of batch jobs via an automated process (i.e., scheduler or other sources) and each of the associated userids. Determine any other scheduled batch jobs on the system.

From an ISPF Command Shell enter:

RLIST SURROGAT *

If each batch job userid used for batch submission by a Job Scheduler (e.g., CONTROL-M, CA-7, CA-Scheduler, etc.) is defined as an execution-userid in a SURROGAT resource class profile, this is not a finding.

From an ISPF Command Shell enter:
RLIST SURROGAT <surrogat-userid> ALL

If the Job Scheduler userids (i.e., surrogate-userid) are permitted surrogate authority to the appropriate SURROGAT profiles, this is not a finding.

Fix Text: Configure each batch job userid used for batch submission by a Job Scheduler (e.g., CONTROL-M, CA-7, CA-Scheduler, etc.) is defined as an execution-userid in a SURROGAT resource class profile. For example:

```
RDEFINE SURROGAT execution-userid.SUBMIT UACC(NONE)  
OWNER(execution-userid)
```

Configure Job Scheduler userids (i.e., surrogate-userid) are permitted surrogate authority to the appropriate SURROGAT profiles. For example:

```
PERMIT execution-userid.SUBMIT CLASS(SURROGAT)  
ID(surrogate-userid) ACCESS(READ)
```

CCI: CCI-000213

CCI: CCI-002233

Group ID (Vulid): V-223673

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223673r853579_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000250](#)

Rule Title: IBM RACF batch jobs must be protected with propagation control.

Legacy ID: SV-107155

Legacy ID: V-98051

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-000326-GPOS-00126

Check Content:

Refer to a list all Multiple User Access Systems in use on this system. These are systems that run in a single address space, but allow multiple users to sign on to them (e.g., CICS regions, Session Managers, etc.). For each region, also include corresponding userids, profiles, data management files, and a brief description (of each region).

Refer to the documentation of the processes used for submission of batch jobs via an automated process (i.e., scheduler or other sources) and each of the associated userids.

If the submission of batch jobs via an automated process (e.g., job scheduler, job submission started task, etc.) is being utilized, and/or Multiple User Single Address Space Systems (MUSASS) capable of submitting batch jobs are active on this system and the following items are in effect, this is not a finding.

The PROPCNTL resource class is active.

A PROPCNTL resource class profile is defined for each userid associated with a job scheduler (e.g., CONTROL-M, CA-7, etc.) and a MUSASS able to submit batch jobs (e.g., CA-ROSCOE, etc.).

Fix Text: Add a PROPCNTL profile for each userid associated with a job scheduler (e.g., CONTROL-M, CA-7, etc.) or a MUSASS able to submit batch jobs (e.g., CA-ROSCOE, etc.).

A sample command is shown here:

```
RDEF PROPCNTL controlm UACC(NONE) OWNER(ADMIN)
```

CCI: CCI-000213

CCI: CCI-002233

Group ID (Vulid): V-223674

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223674r604139_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000260](#)

Rule Title: IBM RACF must limit Write or greater access to SYS1.IMAGELIB to system programmers only.

Legacy ID: SV-107157

Legacy ID: V-98053

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:

Execute a dataset list of access for SYS1.IMAGELIB.

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

-The ACP data set rules for SYS1.IMAGELIB do not restrict WRITER or greater access to only systems programming personnel.

-The ACP data set rules for SYS1.IMAGELIB do not specify that all (i.e., failures and successes) WRITER or greater access will be logged.

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

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

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

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-223675

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223675r853580_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000270](#)

Rule Title: IBM RACF must limit Write or greater access to SYS1.SVCLIB to appropriate authorized users.

Legacy ID: SV-107159

Legacy ID: V-98055

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

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

Check Content:

Execute a dataset list of access for SYS1.SVCLIB.

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

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

-ESM data set rules for SYS1.SVCLIB restrict WRITE or greater access to only z/OS systems programming personnel.

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

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

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223676

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223676r853581_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000280](#)

Rule Title: IBM RACF must limit Write or greater access to SYS1.LPALIB to system programmers only.

Legacy ID: V-98057

Legacy ID: SV-107161

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

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

Check Content:

Execute a dataset list of access for SYS1.LPALIB.

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

-The ESM data set rules for SYS1.LPALIB do not restrict WRITE or greater access to only z/OS systems programming personnel.

-The ESM data set rules for SYS1.LPALIB do not specify that all (i.e., failures and successes) WRITE or greater access will be logged.

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

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

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223677

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223677r853582_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000290](#)

Rule Title: IBM z/OS libraries included in the system REXXLIB concatenation must be properly protected.

Legacy ID: V-98059

Legacy ID: SV-107163

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, 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 ESM dataset rules for libraries in the REXXLIB concatenation restrict GLOBAL read access, this is not a finding.

If ESM data set rules for libraries in the REXXLIB concatenating restrict WRITE or Greater access to z/OS system Programmers, 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
- 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 dataset rules to limit WRITE or greater access to libraries included in the system REXXLIB concatenation to system programmers only.

Configure ESM dataset rules allow READ access to only appropriate Started Tasks and Auditors.

Configure ESM dataset rules to log UPDATE and/or ALTER access (i.e., successes and failures).

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223678

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223678r853583_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000300](#)

Rule Title: IBM RACF must limit write or greater access to all LPA libraries to system programmers only.

Legacy ID: V-98061

Legacy ID: SV-107165

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

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

Check Content:

From Any ISPF input line, enter:
TSO ISRDDN LPA.

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

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

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

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

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223679
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223679r868811_rule
Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000310](#)

Rule Title: IBM RACF must limit Write or greater access to libraries containing EXIT modules to system programmers only.

Legacy ID: V-98063

Legacy ID: SV-107167

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

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

Check Content:

Examine the system for active exit modules. The system administrator may have to 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 WRITE or greater access to only z/OS systems programming personnel, this is not a finding.

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

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

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

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223680

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223680r853585_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000320](#)

Rule Title: IBM RACF must limit WRITE or greater access to all system-level product installation libraries to system programmers.

Legacy ID: V-98065

Legacy ID: SV-107169

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

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

Check Content:

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

The data set name and associated SREL for each SMP/E CSI utilized to maintain this system.
The data set name of all SMP/E TLIBs and DLIBs used for installation and production support.
A comprehensive list of the SMP/E DDDEFs for all CSIs may be used if valid.

If the ESM data set rules for system-level product installation libraries (e.g., SMP/E CSIs) do not restrict WRITE or greater access to only z/OS systems programming personnel this is a finding.

If any of 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-223681

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223681r853586_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000330](#)

Rule Title: IBM RACF must limit access to SYSTEM DUMP data sets to system programmers only.

Legacy ID: V-98067

Legacy ID: SV-107171

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

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

Check Content:

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

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

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

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

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

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

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223682

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223682r853587_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000340](#)

Rule Title: IBM RACF must limit WRITE or greater access to all APF-authorized libraries to system programmers only.

Legacy ID: V-98069

Legacy ID: SV-107173

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, SRG-OS-000324-GPOS-00125

Check Content:

From Any ISPF input line, enter TSO ISRDDN APF.

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

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

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

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

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

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

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223683

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223683r853588_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000350](#)

Rule Title: IBM RACF access to SYS1.LINKLIB must be properly protected.

Legacy ID: V-98071

Legacy ID: SV-107175

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

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000259-GPOS-00100, SRG-OS-000324-GPOS-00125, SRG-OS-000362-GPOS-00149

Check Content:

Execute a dataset list of access to SYS1.LINKLIB.

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

If data set rules for SYS1.LINKLIB do not restrict READ, UPDATE, and ALTER access to only systems programming personnel, this is a finding.

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

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

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

Fix Text: Configure the ESM rules for SYS1.LINKLIB to 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-223684

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223684r767083_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000360](#)

Rule Title: The IBM RACF System REXX IRRPWREX security data set must be properly protected.

Legacy ID: SV-107177

Legacy ID: V-98073

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.

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.

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

GPOS-00100

Check Content:

Refer to the zOS system REXXLIB concatenation found in SYS1. PARMLIB (AXR) for the data set that contains the REXX for Password exit named IRRPWREX and the defined AXRUSER.

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

- RACF data set access authorizations restrict READ to AXRUSER, z/OS systems programming personnel, security personnel, and auditors.
- RACF data set access authorizations restrict UPDATE to security personnel using a documented change management procedure to provide a mechanism for access and revoking of access after use.
- All (i.e., failures and successes) data set access authorities (i.e., READ, UPDATE, and CONTROL) is logged.
- RACF data set access authorizations specify UACC(NONE) and NOWARNING.

Fix Text: Configure read access to be restricted to security administrators, systems programmers, and auditors.

Establish a procedure documented with the ISSM that defines a change management process to provide mechanism for granting Update access to security administrators on an exception basis. The process should contain procedures to revoke access when documented update is completed.

Configure all failures and successes data set access authorities for RACF data set that contains the Password exit to be logged.

Examples:

```
ad 'sys3.racf.rexxlib.**' uacc(none) owner(sys3) -  
audit(all(read))
```

```
Permit 'sys3.racf.rexxlib.**' id(<syspsmpl> <secasmpl> <smplsmp1> AXRUSER) acc(r)
```

```
Permit 'sys3.racf.rexxlib.**' id(<secasmpl>) acc(u)
```

CCI: CCI-000213

CCI: CCI-001084

CCI: CCI-001499

Group ID (Vulid): V-230209

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-230209r767105_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000365](#)

Rule Title: The IBM RACF System REXX IRRPHREX security data set must be properly protected.

Legacy ID: SV-71007

Legacy ID: V-56747

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 z/OS system REXXLIB concatenation found in SYS1.PARMLIB (AXR) for the data set that contains the REXX for Password exit named IRRPHREX and the defined AXRUSER.

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

- RACF data set access authorizations restrict READ to AXRUSER, z/OS systems programming personnel, security personnel, and auditors.
- RACF data set access authorizations restrict UPDATE to security personnel using a documented change management procedure to provide a mechanism for access and revoking of access after use.
- All (i.e., failures and successes) data set access authorities (i.e., READ, UPDATE, and CONTROL) is logged.
- RACF data set access authorizations specify UACC(NONE) and NOWARNING.

Fix Text: Configure read access to be restricted to security administrators, systems programmers, and auditors.

Establish a procedure documented with the ISSM that defines a change management process to provide mechanism for granting Update access to security administrators on an exception basis. The process should contain procedures to revoke access when documented update is completed.

Configure all failures and successes data set access authorities for RACF data set that contains the Password exit to be logged.

Examples:

```
ad 'sys3.racf.rexxlib.**' uacc(none) owner(sys3) -  
audit(all(read))
```

```
Permit 'sys3.racf.rexxlib.**' id(<syspsmpl> <secasmpl> <smplsmp> AXRUSER) acc(r)
```

```
Permit 'sys3.racf.rexxlib.**' id(<secasmpl>) acc(u)
```

CCI: CCI-000213

Group ID (Vulid): V-223685

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223685r853589_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000370](#)

Rule Title: IBM RACF security data sets and/or databases must be properly protected.

Legacy ID: SV-107179

Legacy ID: V-98075

Vulnerability Discussion: The External Security Manager (ESM) database files contain all access control information for the operating system environment and system resources. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

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

Check Content:

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

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

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

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

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

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

CCI: CCI-000213

CCI: CCI-001084

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223686

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223686r868813_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000380](#)

Rule Title: IBM RACF must limit access to data sets used to back up and/or dump SMF collection files to appropriate users and/or batch jobs that perform SMF dump processing.

Legacy ID: SV-107181

Legacy ID: V-98077

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

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

Check Content:

Obtain the procedures and collection specifics for SMF datasets and backup.

If the ESM data set rules for the SMF dump/backup files do not restrict WRITE or greater to authorized DISA and 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 SMF dump/backup files do not specify that all (i.e., failures and successes) WRITE or greater 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 datasets used to backup and/or dump SMF collection files.

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

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

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

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

CCI: CCI-000213

CCI: CCI-001314

CCI: CCI-002235

Group ID (Vulid): V-223687

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223687r869469_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000390](#)

Rule Title: IBM RACF must limit all system PROCLIB data sets to system programmers only.

Legacy ID: V-98079

Legacy ID: SV-107183

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

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

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

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

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

MSTJCL00

```
//MSTJCL00 JOB MSGLEVEL=(1,1),TIME=1440
//EXEC PGM=IEEMB860,DPRTY=(15,15)
//STCINRDR DD SYSOUT=(A,INTRDR)
//TSOINRDR DD SYSOUT=(A,INTRDR)
//IEFPDSI DD DSN=SYS3.PROCLIB,DISP=SHR <<<===
//DD DSN=SYS2.PROCLIB,DISP=SHR <<<===
//DD DSN=SYS1.PROCLIB,DISP=SHR <<<===
//SYSUADS DD DSN=SYS1.UADS,DISP=SHR
//SYSLBC DD DSN=SYS1.BROADCAST,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-223688

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223688r853592_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000400](#)

Rule Title: IBM RACF must limit access to System page data sets (i.e., PLPA, COMMON, and LOCALx) to system programmers.

Legacy ID: V-98081

Legacy ID: SV-107185

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

LOCALx).

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

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

Fix Text: Configure the ESM data set rules for system page data sets (PLPA, COMMON, and LOCAL) to restrict access to only systems programming personnel. Auditors may be allowed READ Access as approved by the ISSM.

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223689

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223689r853595_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000410](#)

Rule Title: IBM z/OS MCS consoles access authorization(s) for CONSOLE resource(s) must be properly protected.

Legacy ID: V-98083

Legacy ID: SV-107187

Vulnerability Discussion: 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.

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

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

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

Check Content:

Verify the CONSOLxx member of SYS1.PARMLIB.console is defined to RACF with a corresponding profile in the CONSOLE resource class.

If each console is defined to RACF with a corresponding profile in the CONSOLE resource class, this is not a finding.

If the userid 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: Define all MCS consoles to the CONSOLE resource class and configure READ access to be limited to operators and system programmers.

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

Each console defined in the CONSOLxx parmlib member is defined to RACF with a corresponding profile in the CONSOLE resource class. See the IBM zOS OPERATIONS AND PLANNING guide for further information.

Each CONSOLE profile is defined with UACC(NONE).

Example:

```
RDEF CONSOLE MMDMST UACC(NONE) OWNER(syspsmpl)
RDEF CONSOLE MMD041 UACC(NONE) OWNER(syspsmpl)
RDEF CONSOLE MMDSCN UACC(NONE) OWNER(syspsmpl)
RDEF CONSOLE ** UACC(NONE) OWNER(syspsmpl) DATA(** represents all consoles not
specifically defined)
```

Do not permit any user or group access to the ** profile. If a new console is added to the CONSOLxx member it will be covered by this profile and a subsequent error will display in the log, which will allow identification of the undefined console.

The userid associated with each console will have READ access to the corresponding resource defined in the CONSOLE resource class. A sample command file to accomplish this is shown here:

```
PE MMDMST CL(CONSOLE) ID(mmdmst)
PE MMDSCN CL(CONSOLE) ID(mmdscn)
PE MMD041 CL(CONSOLE) ID(mmd041)
```

Access authorization for CONSOLE resources restricts READ access to operations and system

programming personnel or authorized personnel. A sample command file showing a permission of READ access for sysprogs and operators is shown here:

```
PE MMDMST CL(CONSOLE) ID(syspsmpl opersmpl)
PE MMDSCN CL(CONSOLE) ID(syspsmpl opersmpl)
PE MMD041 CL(CONSOLE) ID(syspsmpl opersmpl)
```

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223690

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223690r853596_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000420](#)

Rule Title: IBM RACF must limit WRITE or greater access to the JES2 System data sets (e.g., Spool, Checkpoint, and Initialization parameters) to system programmers only.

Legacy ID: V-98085

Legacy ID: SV-107189

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

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

Check Content:

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

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

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

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

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

Configure WRITE or greater access to JES2 System datasets (spool, checkpoint, and parmlib datasets) to be limited to system programmers only.

Access other than this should be documented and approved by the ISSO (for example, all SYS1.HASP* data sets).

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223691

Group Title: SRG-OS-000324-GPOS-00125

Rule ID: SV-223691r877392_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000430](#)

Rule Title: The IBM z/OS IEASYMUP resource must be protected in accordance with proper security requirements.

Legacy ID: V-98087

Legacy ID: SV-107191

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

Check Content:

From the ISPF Command Shell enter:

Search all Class(Facility) MASK(ieasymup)

For each entity found enter:

RL facility <entity>

If RACF resources are defined with a default access of NONE, this is not a finding.

If RACF resource access authorizations restrict UPDATE and/or greater access to appropriate personnel (i.e., DASD administrators, Tape Library personnel, and system programming personnel), this is not a finding.

If RACF resource logging requirements are specified for UPDATE and/or greater access, this is not a finding.

Fix Text: Ensure that the System level symbolic resources are defined to the FACILITY resource class and protected. UPDATE access to the System level symbolic resources are limited to System Programmers, DASD Administrators, and/or Tape Library personnel. All access is logged. Ensure the guidelines for the resources and/or generic equivalent are followed.

Limit access to the IEASYMUP resources to above personnel with UPDATE and/or greater access.

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

```
rdef facility ieasymup.* uacc(none) owner(admin) -  
audit(all(read)) -  
data('protected per acp00350')  
rdef facility ieasymup.symbolname uacc(none) owner(admin) -  
audit(all(read)) -  
data('protected per acp00350')
```

```
pe ieasymup.symbolname cl(facility) id(<dasdsmpl) acc(u)  
pe ieasymup.symbolname cl(facility) id(<syspsmpl) acc(u)  
pe ieasymup.symbolname cl(facility) id(<tapesmpl) acc(u)
```

CCI: CCI-002235

Group ID (Vulid): V-223692

Group Title: SRG-OS-000326-GPOS-00126

Rule ID: SV-223692r853598_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000440](#)

Rule Title: The IBM RACF JES(BATCHALLRACF) SETROPTS value must be set to JES(BATCHALLRACF).

Legacy ID: SV-107193

Legacy ID: V-98089

Vulnerability Discussion: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned by the organizations.

Some programs and processes are required to operate at a higher privilege level and therefore should be excluded from the organization-defined software list after review.

Check Content:

From ISPF Command Shell enter:
SETRopts List

If the JES(BATCHALLRACF) is enabled then the message "JES-BATCHALLRACF OPTION IS ACTIVE" will be displayed, this is not a finding.

If the message "JES-BATCHALLRACF OPTION IS INACTIVE" is displayed, this is a finding.

Fix Text: Configure JES(BATCHALLRACF) SETROPTS value to be set to JES(BATCHALLRACF). This specifies that JES is to test for a userid and password on the job statement or for propagated RACF identification information for all batch jobs.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including a status of JES BATCHALLRACF.

JES BATCHALLRACF is activated with the command SETR JES(BATCHALLRACF).

CCI: CCI-002233

Group ID (Vulid): V-223693

Group Title: SRG-OS-000326-GPOS-00126

Rule ID: SV-223693r853599_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000460](#)

Rule Title: The IBM z/OS JES(XBMALLRACF) SETROPTS value must be set to JES(XBMALLRACF).

Legacy ID: SV-107197

Legacy ID: V-98093

Vulnerability Discussion: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned by the organizations.

Some programs and processes are required to operate at a higher privilege level and therefore should be excluded from the organization-defined software list after review.

Check Content:

From the ISPF Command Shell enter:
SETRopts List

If the JES(XBMALLRACF) is enabled then the message "JES-XBMALLRACF OPTION IS ACTIVE" will be displayed, this is not a finding.

If the message "JES-XBMALLRACF OPTION IS INACTIVE" is displayed, this is a finding.

Fix Text: Configure JES(XBMALLRACF) SETROPTS value to be set to JES(XBMALLRACF). This specifies that JES is set to test for a userid and password on the job statement or for propagated RACF identification information for all jobs run under the execution batch monitor.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including a status of JES-XBMALLRACF.

XBMALLRACF is activated with the command SETR XBMALLRACF.

CCI: CCI-002233

Group ID (Vulid): V-223694

Group Title: SRG-OS-000327-GPOS-00127

Rule ID: SV-223694r853600_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000470](#)

Rule Title: IBM RACF OPERAUDIT SETROPTS value must set to OPERAUDIT.

Legacy ID: SV-107199

Legacy ID: V-98095

Vulnerability Discussion: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Check Content:

From the ISPF Command Shell enter:
SETRopts List

If the OPERAUDIT value is listed as one of the ATTRIBUTES, this is not a finding.

If the OPERAUDIT value is not listed as one of the ATTRIBUTES, this is a finding.

Fix Text: NOTE: The RACF AUDITOR attribute is required in order to specify SETROPTS OPERAUDIT and also to display the OPERAUDIT attribute with the SETROPTS LIST command.

Configure the OPERAUDIT SETROPTS value to be set to OPERAUDIT. This specifies that RACF logs all actions such as accesses to resources and commands for a user who has operations or group operations attribute.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including a list of ATTRIBUTES.

Logging of all actions, such as accesses to resources and commands, allowed only because a user has the OPERATIONS or group-OPERATIONS attribute is activated with the command SETR OPERAUDIT.

CCI: CCI-002234

Group ID (Vulid): V-223695

Group Title: SRG-OS-000021-GPOS-00005

Rule ID: SV-223695r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000480](#)

Rule Title: The IBM RACF PASSWORD(REVOKE) SETROPTS value must be specified to revoke the userid after three invalid logon attempts.

Legacy ID: SV-107201

Legacy ID: V-98097

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

Check Content:

From the ISPF Command Shell enter:
SETRopts List

If the PASSWORD(REVOKE) value shows "AFTER <n> CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS, A USERID WILL BE REVOKED." where <n> is either "1" or "2", this is not a finding.

If the PASSWORD(REVOKE) value is not enabled and is not set to either "1" or "2", this is a finding.

Fix Text: Ensure that PASSWORD(REVOKE) SETROPTS value is set to "1" or "2". This specifies the number of consecutive incorrect password attempts RACF allows before it revokes the USERID on the next incorrect attempt. If you specify REVOKE, ensure INITSTATS are in effect.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including PASSWORD REVOKE.

Setting the password REVOKE to "2" invalid attempts activated with the command SETR PASSWORD(REVOKE(2)).

CCI: CCI-000044

Group ID (Vulid): V-223696

Group Title: SRG-OS-000329-GPOS-00128

Rule ID: SV-223696r853602_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000490](#)

Rule Title: The IBM RACF PASSWORD(REVOKE) SETROPTS value must be set to automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts occur.

Legacy ID: V-98099

Legacy ID: SV-107203

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

Check Content:

From the ISPF Command Shell enter:
SETRopts List

If the PASSWORD(REVOKE) value shows "AFTER <n> CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS, A USERID WILL BE REVOKED." where <n> is either "1" or "2", this is not a finding.

If the PASSWORD(REVOKE) value is not enabled and is not set to either "1" or "2", this is a finding.

Fix Text: Ensure that PASSWORD(REVOKE) SETROPTS value is set to "1" or "2". This specifies the number of consecutive incorrect password attempts RACF allows before it revokes the USERID on the next incorrect attempt. If REVOKE is specified, ensure INITSTATS are in effect.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including PASSWORD REVOKE.

Set the password REVOKE to "2" invalid attempts activated with the command SETR PASSWORD(REVOKE(2)).

CCI: CCI-002238

Group ID (Vulid): V-223697

Group Title: SRG-OS-000063-GPOS-00032

Rule ID: SV-223697r853603_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000500](#)

Rule Title: IBM z/OS SYS1.PARMLIB must be properly protected.

Legacy ID: V-98101

Legacy ID: SV-107205

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

SYS1.PARMLIB contains the parameters that control audit configuration. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.

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 dataset list of access to SYS1.PARMLIB.

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

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

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

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

If data set rules for SYS1.PARMLIB do not specify that all (i.e., failures and successes) UPDATE and/or ALTER 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 WRITE or greater 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 WRITE or greater 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-223699

Group Title: SRG-OS-000468-GPOS-00212

Rule ID: SV-223699r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000520](#)

Rule Title: The IBM RACF SETROPTS SAUDIT value must be specified.

Legacy ID: V-98105

Legacy ID: SV-107209

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Check Content:

From the ISPF Command Shell enter:

SETROPTS LIST

If the SAUDIT value is listed as one of the ATTRIBUTES, this is not a finding.

If the NOSAUDIT value is listed as one of the ATTRIBUTES, 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 in the example below:

Note: that in order to set or list the SAUDIT value, the RACF AUDITOR attribute is required. Reference the documentation for the SETROPTS command in the RACF Command Language Reference.

The RACF Command SETR LIST will show the status of RACF Controls including the value for SAUDIT.

SAUDIT is activated and set to the required value by issuing the command SETR SAUDIT.

CCI: CCI-000172

Group ID (Vulid): V-223700

Group Title: SRG-OS-000255-GPOS-00096

Rule ID: SV-223700r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000530](#)

Rule Title: The IBM RACF REALDSN SETROPTS value must be specified.

Legacy ID: V-98107

Legacy ID: SV-107211

Vulnerability Discussion: Without information that establishes the identity of the subjects (i.e., users or processes acting on behalf of users) associated with the events, security personnel cannot determine responsibility for the potentially harmful event.

Check Content:

From the ISPF Command Shell enter:
SETRopts list

If the REALDSN is enabled then the message "REAL DATA SET NAMES OPTION IS ACTIVE" will be displayed, this is not a finding.

If the message "REAL DATA SET NAMES OPTION IS INACTIVE" is displayed, this is a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Configure control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including the value for the REALDSN Option.

REALDSN is ACTIVATED by issuing the command SETR REALDSN.

CCI: CCI-001487

Group ID (Vulid): V-223701

Group Title: SRG-OS-000057-GPOS-00027

Rule ID: SV-223701r853604_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000540](#)

Rule Title: IBM z/OS must limit access for SMF collection files (i.e., SYS1.MANx) to appropriate users and/or batch jobs that perform SMF dump processing.

Legacy ID: V-98109

Legacy ID: SV-107213

Vulnerability Discussion: SMF data collection is the system activity journaling facility of the z/OS system. Unauthorized access could result in the compromise of logging and recording of the operating system environment, ESM, and customer data.

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit operating system activity.

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

Check Content:

Refer to the SMFPRMxx member in SYS1.PARMLIB. Determine the SMF and/or Logstream dataset name.

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

The ESM data set rules for the SMF data collection files (e.g., SYS1.MAN* or IFASMF.SYS1.*) restrict WRITE or greater access to only z/OS systems programming personnel.

The ESM data set rules for the SMF data collection files (e.g., SYS1.MAN* or IFASMF.SYS1.*) restrict UPDATE access to z/OS systems programming personnel, and/or

batch jobs that perform SMF dump processing and others approved by ISSM.

The ESM data set rules for the SMF data collection files (e.g., SYS1.MAN* or IFASMF.SYS1.*) restrict READ access to auditors and others approved by the ISSM.

The ESM data set rules for SMF data collection files (e.g., SYS1.MAN* or IFASMF.SYS1.*) specify that all (i.e., failures and successes) UPDATE and/or ALTER access are logged.

Fix Text: Configure WRITE and above access to SMF collection files to be 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.

Configure READ access to be limited to auditors. READ access may be granted to others as determined by the ISSM.

Access to other users specified must be documented in a security plan.

Ensure the accesses are being 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-223702

Group Title: SRG-OS-000364-GPOS-00151

Rule ID: SV-223702r853605_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000550](#)

Rule Title: IBM RACF SETROPTS RVARYPW values must be properly set.

Legacy ID: V-98111

Legacy ID: SV-107215

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:

From the ISPF Command Shell enter:

SETROPTS LIST

If the "INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT" message for both the SWITCH and STATUS functions, this is not a finding.

Fix Text: Configure RACF ensure that the RVARYPW passwords are specified and conform to password requirements documented in RACF0460. The ISSO will evaluate the impact associated with implementation of the control option and develop a plan of action to implement the control option as required.

A sample command for setting both the SWITCH and STATUS passwords are shown here:

```
SETR RVARYPW(SWITCH(Wxy$8Pqu) STATUS(pbZ0@wL2))
```

CCI: CCI-001813

Group ID (Vulid): V-223703

Group Title: SRG-OS-000480-GPOS-00229

Rule ID: SV-223703r877377_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000560](#)

Rule Title: IBM RACF must define WARN = NO on all profiles.

Legacy ID: V-98113

Legacy ID: SV-107217

Vulnerability Discussion: Failure to restrict system access to authenticated users negatively impacts operating system security.

Check Content:

Review all Dataset and resource profiles in the RACF database.

If any are not defined with WARN = NO, this is a finding.

Fix Text: Define each dataset and resource profile with WARN = NO

CCI: CCI-000366

Group ID (Vulid): V-223704

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223704r604139_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000570](#)

Rule Title: The IBM RACF PROTECTALL SETROPTS value specified must be properly set.

Legacy ID: SV-107219

Legacy ID: V-98115

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

Configuration settings are the set of parameters that can be changed in hardware, software, or

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

Check Content:

From the ISPF Command Shell enter:
SETROPTS LIST

If the SETROPTS values for PROTECTALL is ACTIVE and set to FAIL, this is not a finding.

If the SETROPTS PROTECTALL parameter is set to NOPROTECTALL or PROTECTALL(WARNING), this is a finding.

Additional analysis may be required to determine whether this finding should be downgraded to a Category II or remain a Category I.

Example of a Category I finding where not a further analysis is required:

Control Options: SETROPTS NOPROTECTALL

Example of a possible Category I finding requiring additional analysis:

Control Options: SETROPTS PROTECTALL(WARNING)

PROTECTALL(WARNING) allows access to a data set only if it is not at protected by a profile in the DATASET resource class. Therefore if all sensitive data sets are properly protected by profiles in the DATASET resource class, PROTECTALL(WARNING) will not at allow unauthorized access. This situation allows for a downgrade to a Category II.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including the value for the PROTECTALL Option.

PROTECTALL is ACTIVATED and set to FAIL by issuing the command SETR PROTECTALL(FAIL).

CCI: CCI-000366

Group ID (Vulid): V-223705

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223705r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000580](#)

Rule Title: The IBM RACF GRPLIST SETROPTS value must be set to ACTIVE.

Legacy ID: SV-107221

Legacy ID: V-98117

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

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

Check Content:

From the ISPF Command Shell enter:

SETROPTS LIST

If the GRPLIST is enabled then the message "LIST OF GROUPS ACCESS CHECKING IS ACTIVE." will be displayed, this is not a finding.

If the message indicates that LIST OF GROUPS is NOT ACTIVE, this is a finding.

Fix Text: Configure the GRPLIST SETROPTS value to be set to ACTIVE.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including a status of GRPLIST.

List of Groups Checking is activated with the command SETR GRPLIST.

CCI: CCI-000366

Group ID (Vulid): V-223706

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223706r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000590](#)

Rule Title: The IBM RACF RETPD SETROPTS value specified must be properly set.

Legacy ID: SV-107223

Legacy ID: V-98119

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

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

Check Content:

From the ISPF Command Shell enter:
SETROPTS LIST

If the RETPD is enabled then the message "SECURITY RETENTION PERIOD IN EFFECT IS NEVER-EXPIRES DAYS" will be displayed, this is not a finding.

If the RETPD value is not set to "NEVER-EXPIRES", 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 in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including the value for the RETPD (Retention Period) Option.

RETPD is activated and set to the required value by issuing the command SETR RETPD(99999).

CCI: CCI-000366

Group ID (Vulid): V-223707

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223707r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000600](#)

Rule Title: The IBM RACF TAPEDSN SETROPTS value specified must be properly set.

Legacy ID: SV-107225

Legacy ID: V-98121

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

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

Check Content:

From the ISPF Command Shell enter:
SETROPTS LIST

If the TAPEDSN is enabled then the message "TAPE DATA SET PROTECTION IS ACTIVE" will be displayed, this is not a finding.

NOTE 1: TAPEDSN should be active for domains without a tape management product.

NOTE 2: For domains running CA 1, Computer Associates recommends that TAPEDSN be active and CA 1 parameter OCEOV be set to OFF.

If the TAPEDSN value is set to INACTIVE, 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 in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including the value for the TAPEDSN Option.

TAPEDSN is ACTIVATED by issuing the command SETR TAPEDSN.

CCI: CCI-000366

Group ID (Vulid): V-223708

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223708r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000610](#)

Rule Title: The IBM RACF WHEN(PROGRAM) SETROPTS value specified must be active.

Legacy ID: V-98123

Legacy ID: SV-107227

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

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

Check Content:

From the ISPF Command Shell enter:
SETROPTS LIST

If the WHEN(PROGRAM) value is listed as one of the ATTRIBUTES, this is not a finding.

If the NOWHEN(PROGRAM) value is listed as one of the ATTRIBUTES, 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 in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including the value for the WHEN(PROGRAM) Option.

WHEN(PROGRAM) is ACTIVATED by issuing the command SETR WHEN(PROGRAM).

CCI: CCI-000366

Group ID (Vulid): V-223709

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223709r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000620](#)

Rule Title: IBM RACF use of the AUDITOR privilege must be justified.

Legacy ID: V-98125

Legacy ID: SV-107229

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

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

Check Content:

From the ISPF Command Shell enter:

ListUser *

If authorization to the SYSTEM AUDITOR attribute is restricted to auditing and/or security personnel, this is not a finding.

If at minimum, any users connected to sensitive system dataset HLQ (e.g., SYS1, SYS2, etc.) groups or general resource owning groups with the Group-AUDITOR attribute are Auditor and/or Security personnel, this is not a finding.

Otherwise, Group-AUDITOR is allowed.

Fix Text: Review all USERIDs with the AU (Manual) - Review all USERIDs with the AUDITOR attribute. Ensure documentation providing justification for access is maintained and filed with the ISSO, and that unjustified access is removed.

The AUDITOR attribute is removed from a user with the command: ALU <userid>
NOAUDITOR.

To remove the Group-Auditor attribute:

CO <user> GROUP(<groupname>) NOAUDITOR

CCI: CCI-000366

Group ID (Vulid): V-223710

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223710r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000630](#)

Rule Title: The IBM RACF database must be on a separate physical volume from its backup and recovery datasets.

Legacy ID: V-98127

Legacy ID: SV-107231

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:

Execute the RACDST report from DSMON Utility using 'RACF PRIMARY' and 'RACF BACKUP' as selection criteria.

If the security database and its backup exist on the same volume, this is a finding.

Fix Text: Identify the ACP 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 ACP files.

CCI: CCI-000366

Group ID (Vulid): V-223711

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223711r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000640](#)

Rule Title: The IBM RACF database must be backed up on a scheduled basis.

Legacy ID: V-98129

Legacy ID: SV-107233

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 that procedures exist to back up the security data base and files. Have the system administrator identify the dataset names and frequency of the backups.

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: Develop procedures to back up all ACP files needed for recovery on a scheduled basis.

Identify the ACP database and ensure that documented processes are in place to back up its contents on a regularly scheduled basis.

At a minimum, this should include 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-223712

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223712r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000650](#)

Rule Title: IBM z/OS Batch job user IDs must be properly defined.

Legacy ID: V-98131

Legacy ID: SV-107235

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 documentation of the processes used for submission of batch jobs via an automated process (i.e., scheduler or other sources) and each of the associated user IDs.

From the ISPF COMMAND INPUT screen enter:
LISTUSER(each identified batch job)

The following USERID record fields/attributes must be specified:

NAME
PROTECTED

No USERID has the LAST-ACCESS field set to UNKNOWN.

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

If either of the USERID record fields/attributes (NAME and/or PROTECTED) are blank and/or the LAST ACCESS field is set to unknown, this is a finding.

Fix Text: Ensure the following:

Associated USERIDs are defined for all batch jobs and documentation authorizing access to system resources is maintained and implemented.

Set up the userids with the RACF PROTECTED attribute. A sample RACF command to accomplish is shown here: ALU <execution-userid> NOPASSWORD NOOIDCARD.

CCI: CCI-000366

Group ID (Vulid): V-223713

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223713r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000660](#)

Rule Title: IBM RACF use of the RACF SPECIAL Attribute must be justified.

Legacy ID: V-98133

Legacy ID: SV-107237

Vulnerability Discussion: 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 the ISPF Command Shell enter:

ListUser *

If authorization to the SYSTEM SPECIAL attribute is restricted to key systems personnel such as individuals responsible for continuing operations, Storage Management, and emergency recovery, this is not a finding.

If any users connected to sensitive system dataset HLQ (e.g., SYS1, SYS2, ETC) groups with the Group-SPECIAL are key systems personnel, such as individuals responsible for continuing operations, Storage Management, and emergency recovery, this is a finding.

Otherwise, Group-SPECIAL is allowed.

Fix Text: Review all USERIDs with the SPECIAL attribute. Ensure documentation providing justification for access is maintained and filed with the ISSO, and that unjustified access is removed.

For the SYSTEM SPECIAL attribute:

A sample command for removing the SPECIAL attribute is shown here: ALU <userid>
NOSPECIAL.

For the GROUP SPECIAL attribute:

CO <user> GROUP(<groupname>) NOSPECIAL

CCI: CCI-000366

Group ID (Vulid): V-223714

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223714r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000670](#)

Rule Title: IBM RACF assignment of the RACF OPERATIONS attribute to individual userids must be fully justified.

Legacy ID: V-98135

Legacy ID: SV-107239

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:

From the ISPF Command Shell enter:

ListUser *

If authorization to the SYSTEM OPERATIONS attribute is restricted to key systems personnel such as individuals responsible for continuing operations, Storage Management, and emergency recovery, this is not a finding.

If any users connected to sensitive system dataset HLQ (e.g., SYS1, SYS2, ETC) groups with the Group-OPERATIONS are key systems personnel, such as individuals responsible for continuing operations, Storage Management, and emergency recovery, this is a finding.

Otherwise, Group-OPERATIONS is allowed.

Fix Text: Review all USERIDs with the OPERATIONS attribute. Ensure documentation providing justification for access is maintained and filed with the ISSO, and that unjustified access is removed.

A sample command to remove the OPERATIONS attribute from a userid is shown here:

```
ALU <userid> NOOPERATIONS
```

To remove the Group-Operations attribute:

```
CO <user> GROUP(<groupname>) NOOPERATIONS
```

CCI: CCI-000366

Group ID (Vulid): V-223715

Group Title: SRG-OS-000096-GPOS-00050

Rule ID: SV-223715r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000680](#)

Rule Title: IBM z/OS must properly configure CONSOLxx members.

Legacy ID: SV-107241

Legacy ID: V-98137

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. See ACP00292.

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

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

CCI: CCI-000382

Group ID (Vulid): V-223716

Group Title: SRG-OS-000096-GPOS-00050

Rule ID: SV-223716r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000690](#)

Rule Title: IBM z/OS must properly protect MCS console userid(s).

Legacy ID: SV-107243

Legacy ID: V-98139

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:

Refer to IEASYS00 to determine correct CONSOLxx member.

Examine the CONSOLxx member.

Verify that the MCS console userids are properly restricted.

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

Each console defined in the currently active CONSOLxx parmlib member in EXAM.RPT(PARMLIB) is associated with a valid RACF userid.

Each console userid has no special privileges and/or attributes (e.g., SPECIAL, OPERATIONS, etc.).

Each console userid has no accesses to interactive on-line facilities (e.g., TSO, CICS, etc.; excluding VTAM SMCS consoles).

Each console userid will be restricted from accessing all data sets and resources except MVS.MCSOPER.consolename in the OPERCMDS resource class and console name in the

CONSOLE resource class.

Each console userid has the RACF default group that is an appropriate console group profile.

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

NOTE: Execute the JCL in CNTL(IRRUT100) using the RACF console userids as SYSIN input. This report lists all occurrences of these userids within the RACF 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 RACF.

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

Each console defined in the currently active CONSOLxx parmlib member in EXAM.RPT(PARMLIB) is associated with a valid RACF userid.

Each console userid has no special privileges and/or attributes (e.g., SPECIAL, OPERATIONS, etc.).

Each console userid has no accesses to interactive on-line facilities (e.g., TSO, CICS, etc.; excluding VTAM SMCS consoles).

Each console userid 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.

Each console userid has the RACF default group that is an appropriate console group profile.

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

NOTE: Execute the JCL in CNTL(IRRUT100) using the RACF console userids as SYSIN input. This report lists all occurrences of these userids within the RACF database, including data set and resource access lists.

Examples:

```
AG consautolog SUPGROUP(<syspsmpl>) OWNER(<syspsmpl>) -  
DATA(' group for console userids for autolog processing ')
```

```
AG consnoautolog SUPGROUP(<syspsmpl>) OWNER(<syspsmpl>) -  
DATA('group for console userids for no autolog processing')
```

```
AU consname NAME('CONSOLE USERID FOR consname') NOPASSWORD NOOIDCARD -  
DFLTGRP(consautolog) OWNER(consautolog) -  
DATA('ADDED TO SUPPORT THE CHANGE TO LOGON(AUTO) IN CONSOLXX')
```

```
PERMIT MVS.CONTROL.** CL(OPERCMD5) ID(consautolog) ACCESS(READ)  
PERMIT MVS.DISPLAY.** CL(OPERCMD5) ID(consautolog) ACCESS(READ)  
PERMIT MVS.MONITOR.** CL(OPERCMD5) ID(consautolog) ACCESS(READ)  
PERMIT MVS.STOPMN.** CL(OPERCMD5) ID(consautolog) ACCESS(READ)
```

```
PERMIT consname CL(CONSOLE) ID(consname)
```

CCI: CCI-000382

Group ID (Vulid): V-223717

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-223717r822576_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000700](#)

Rule Title: IBM RACF users must have the required default fields.

Legacy ID: SV-107245

Legacy ID: V-98141

Vulnerability Discussion: Ensure that Every USERID is uniquely identified to the system. Within the USERID record, the user's name, default group, the owner, and the user's passdate or phrasedate fields are completed. This will uniquely identify each user. If these fields are not completed for each user, user accountability will become lost.

Check Content:

From a z/OS command screen enter:

```
ListUser *
```

Examine each user entry verify every user is fully identified with all of the following conditions:

-A completed NAME field that can either be traced back to a current DD2875 or a Vendor Requirement (example: A Started Task).

- The presence of the DEFAULT-GROUP and OWNER fields.
- The PASSDATE field or the PHRASEDATE field accordingly is not set to N/A excluding users with the PROTECTED attribute.

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

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

Fix Text: Review all USERID definitions to ensure required information is provided. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes listed in this PDI. The following are sample commands to correct this vulnerability.

- To Add a NAME to a userid with the command ALU <userid> NAME('lastname, firstname').
- Every user will be assigned a default group by default. A sample command to reassign a default group is shown here: ALU <userid> DFLTGRP(<newdefaultgroup>). You must first be connected to a group via the RACF CONNECT command before making it a default group.
- A PASSDATE field or a PHRASEDATE field showing 00.000 indicates that a temporary password or password phrase has been assigned but the user has not logged in and set a permanent value. This could indicate that a new userid was recently added or that a userid previously added is unused and should be considered for deletion. The ISSO should investigate and determine if the userid should be deleted or that the new user should be contacted and told to login to set a permanent value.

CCI: CCI-000764

Group ID (Vulid): V-223718

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-223718r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000710](#)

Rule Title: IBM interactive USERIDs defined to RACF must have the required fields completed.

Legacy ID: V-98143

Legacy ID: SV-107247

Vulnerability Discussion: Interactive users are considered to be users of CICS, IMS, TSO/E, NetView, or other products that support logging on at a terminal. Improper assignments of attributes in the LOGONID record for interactive users may allow users excessive privileges resulting in unauthorized access.

Check Content:

From a z/OS command screen enter:

ListUser *

Examine each user entry that has either TSO, CICS, ROSCOE, IMS, or any other products that support logging on at a terminal.

If every user is fully identified with all of the following condition, this is not a finding.

-Each interactive userid has a valid LAST-ACCESS date that does not contain the value UNKNOWN.

-Each interactive userid has PASS-INTERVAL define and set to a value of 60 days.

Note: FTP only process and server to server userids may have PASSWORD(NOINTERVAL) specified. These users must be identified in the FTPUSERS group in the Dialog Process or FTP in the name field. Additionally these users must change their passwords on an annual basis.

Fix Text: Review all interactive USERID definitions to ensure required information is provided. Evaluate the impact of correcting any deficiencies. Develop a plan of action and implement the required changes.

The PASSWORD-INTERVAL for an interactive user must be set to 60 days.

Note: FTP only process and server to server userids may have PASSWORD(NOINTERVAL) specified. These users must be identified in the FTPUSERS group in the Dialog Process or FTP in the name field. Additionally, these users must change their passwords on an annual basis or less.

A sample command to accomplish this is shown here:

```
PW USER(<userid>) INTERVAL(60).
```

The LAST-ACCESS date must be set to a valid date and not to the value UNKNOWN. A sample command to accomplish this is shown here:

```
ALU <userid> RESUME
```

CCI: CCI-000764

Group ID (Vulid): V-223719

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-223719r877336_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000720](#)

Rule Title: IBM z/OS Started Tasks must be properly identified and defined to RACF.

Legacy ID: SV-107249

Legacy ID: V-98145

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

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

Check Content:

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

If each Started task procedure identified has a unique associated userid or STC userid that is unique per product and function, this is not a finding.

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

- All started task userids are connected to a valid STC group ID.
- Only userids associated with STCs are connected to STC group IDs.
- All STC userids are defined with the PROTECTED attribute.

From the ISPF Command Shell enter:

RL STARTED (Alternately execute RACF DSMON utility for the RACSPT report)

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

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

- A generic catch all profile of ** is defined to the STARTED resource class.
- The STC group associated with the ** profile is not granted any explicit data set or resource access authorizations.
- The STC userid associated with the ** profile is not granted any explicit dataset or resource access authorizations and is defined with the RESTRICTED attribute.

Note: Execute the JCL in CNTL(IRRUT100) using the STC group associated with the ** profile as SYSIN input. This report lists all occurrences of this group within the RACF database, including data set and resource access lists.

Execute RACF utility DSMON RACSPT report.

If the ICHRIN03 started procedures table is not maintained to support recovery efforts in the

event the STARTED resource class is deactivated or critical STC profiles are deleted, this is a finding.

If STCs critical to support this recovery effort (e.g., JES2, VTAM, TSO, etc.) are not maintained in ICHRIN03 to reflect the current STARTED resource class profiles, this is a finding.

Fix Text: Define a RACF STARTED Class profile for each Started Proc that maps the proc to a unique userid, or STC userids will be unique per product and function if supported by vendor documentation. This can be accomplished with the sample command:

```
RDEF STARTED <procname>.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
STDATA(USER(<userid>) GROUP(<groupname>) TRACE(YES))
```

A corresponding USERID must be defined with appropriate authority. The "groupname" should be a valid STC group with no interactive users.

CCI: CCI-000764

Group ID (Vulid): V-223721

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-223721r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000740](#)

Rule Title: The IBM RACF Automatic Data Set Protection (ADSP) SETROPTS value must be set to NOADSP.

Legacy ID: V-98149

Legacy ID: SV-107253

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:
SETROPTS LIST

If the ADSP value is NOT IN EFFECT, this is not a finding.

Note: NOADSP is the required setting. In the SETROPTS LIST output this will display as AUTOMATIC DATASET PROTECTION IS NOT IN EFFECT.

If the ADSP value is IN EFFECT, this is a finding.

Fix Text: Configure ADSP SETROPTS value to be set to NOADSP.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

NOADSP is set with the command SETR NOADSP.

CCI: CCI-000764

Group ID (Vulid): V-223722

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-223722r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000750](#)

Rule Title: IBM RACF user accounts must uniquely identify system users.

Legacy ID: V-98151

Legacy ID: SV-107255

Vulnerability Discussion: To assure individual accountability and prevent unauthorized access, organizational users must be individually identified and authenticated.

A group authenticator is a generic account used by multiple individuals. Use of a group authenticator alone does not uniquely identify individual users. Examples of the group authenticator is the UNIX OS "root" user account, the Windows "Administrator" account, the "sa" account, or a "helpdesk" account.

For example, the UNIX and Windows operating systems offer a 'switch user' capability allowing users to authenticate with their individual credentials and, when needed, 'switch' to the administrator role. This method provides for unique individual authentication prior to using a group authenticator.

Users (and any processes acting on behalf of users) need to be uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization, which outlines specific user actions that can be performed on the operating system without identification or authentication.

Requiring individuals to be authenticated with an individual authenticator prior to using a group authenticator allows for traceability of actions, as well as adding an additional level of protection of the actions that can be taken with group account knowledge.

Satisfies: SRG-OS-000104-GPOS-00051, SRG-OS-000109-GPOS-00056, SRG-OS-000125-GPOS-00065, SRG-OS-000121-GPOS-00062

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.

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-000770

CCI: CCI-000804

CCI: CCI-000877

Group ID (Vulid): V-223723

Group Title: SRG-OS-000118-GPOS-00060

Rule ID: SV-223723r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000760](#)

Rule Title: The IBM RACF INACTIVE SETROPTS value must be set to 35 days.

Legacy ID: V-98153

Legacy ID: SV-107257

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 a z/OS command input screen enter:
List SETROpts

If the INACTIVE value is set properly In the message "INACTIVE USERIDS ARE BEING AUTOMATICALLY REVOKED AFTER xxx DAYS.", where xxx is a value "35" or less, this is not a finding.

Fix Text: Configure the INACTIVE SETROPTS value to a value that is "35" or less. INACTIVE specifies the number of days that a USERID can remain unused and still be considered valid.

CCI: CCI-000795

Group ID (Vulid): V-223724

Group Title: SRG-OS-000069-GPOS-00037

Rule ID: SV-223724r868818_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000770](#)

Rule Title: IBM RACF PASSWORD(RULEn) SETROPTS value(s) must be properly set.

Legacy ID: V-98155

Legacy ID: SV-107259

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.

Satisfies: SRG-OS-000069-GPOS-00037, SRG-OS-000078-GPOS-00046

Check Content:

From the ISPF Command Shell enter:
SETRopts

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

At least one PASSWORD(RULE) under "INSTALLATION PASSWORD SYNTAX RULES" is defined with the values shown below:

RULE 1 LENGTH(8) xxxxxxxx

The following options are in effect under "PASSWORD PROCESSING OPTIONS":

"MIXED CASE PASSWORD SUPPORT IS IN EFFECT"
"SPECIAL CHARACTERS ARE ALLOWED."

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

For z/OS release 1.13 and 1.14 PTF UA90720 must be applied.
For z/OS Release 2.1 PTF UA90721 must be applied.

The RACF Command SETR LIST will show the status of RACF Controls including PASSWORD SYNTAX RULES.

Setting the password syntax to all Mixed Case Alphanumeric and Special Characters is activated with the commands:

```
setr password(mixedcase)
setr password(specialchars)
setr password(rule1(length(8) mixedall(1:8))
```

CCI: CCI-000192

CCI: CCI-000205

Group ID (Vulid): V-223725

Group Title: SRG-OS-000070-GPOS-00038

Rule ID: SV-223725r868820_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000780](#)

Rule Title: IBM RACF exit ICHPWX01 must be installed and properly configured.

Legacy ID: SV-107261

Legacy ID: V-98157

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.

Satisfies: SRG-OS-000070-GPOS-00038, SRG-OS-000071-GPOS-00039, SRG-OS-000072-GPOS-00040, SRG-OS-000266-GPOS-00101, SRG-OS-000480-GPOS-00225

Check Content:

From a system console screen issue the following modify command:

```
F AXR,IRRPWREX LIST
```

Review the results of the modify command.

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

- The number of required character types is 4
(assures that at least 1 upper case, 1 lower case, 1 number, and 1 special character is used in Password)
- The user's name cannot be contained in the password
(Only 3 consecutive characters of the user's name are allowed)
- The minimum word length checked is 8
- The user ID cannot be contained in the password
(Only 3 consecutive characters of the user ID are allowed)
- Only 3 unchanged positions of the current password are allowed
(These positions need to be consecutive to cause a failure and this check is not case sensitive)
- No more than 0 pairs of repeating characters are allowed
(This check is not case sensitive)
- A minimum list of 33 restricted prefix strings is being checked:
APPL APR AUG ASDF 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

If the modify command fails or returns the following message in the system log, this is a finding.

IRX0406E REXX exec load file REXXLIB does not contain exec member IRRPWREX.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

For z/OS release 1.12 through z/OS release 2.1 APARs OA43998 and OA43999 must be applied.

Install exit IRRPWREX according to the following guidelines:

REXX Parameter Setting

STIG_Compliant 'yes'

Pwd_minlen 8

numbers '0123456789'

Lower_letters 'abcdefghijklmnopqrstuvwxyZ'

Upper_letters 'ABCDEFGHIJKLMNopQRSTUVWXYZ'

special '\$@#. <+|&!*-%_>?:'

Pwd_allowed_chars numbers||Upper_letters||special

Pwd_req_types 4

Pwd_name_allowed 'no'

Pwd_name_minlen 8

Pwd_name_chars 4

Pwd_min_unique 3

Pwd_min_unique_upper 'yes'

Pwd_max_unchanged 3

Pwd_max_unchanged_upper 'yes'

Pwd_max_unchanged_consecutive 'yes'

Pwd_all_unique 'no'

Pwd_no_consecutive 'no'

Pwd_no_consecutive_upper 'yes'

Pwd_min_new 4

Pwd_userID_allowed 'no'

Pwd_userID_chars 4

Pwd_repeat_chars 0

Pwd_repeat_upper 'yes'

Pwd_dict.0 8 /* Change this as words are added and deleted */

Pwd_dict.1 'IBM'

Pwd_dict.2 'RACF'

Pwd_dict.3 'PASSWORD'

Pwd_dict.4 'PHRASE'

Pwd_dict.5 'SECRET'

Pwd_dict.6 'IBMUSER'

Pwd_dict.7 'SYS1'

Pwd_dict.8 '12345678'

Pwd_dict.9 '99999999'

Pwd_prefix.0 33 /* Change this as values are added and deleted
Pwd_prefix.1 'APPL'
Pwd_prefix.2 'APR'
Pwd_prefix.3 'AUG'
Pwd_prefix.4 'ASDF'
Pwd_prefix.5 'BASIC'
Pwd_prefix.6 'CADAM'
Pwd_prefix.7 'DEC'
Pwd_prefix.8 'DEMO'
Pwd_prefix.9 'FEB'
Pwd_prefix.10 'FOCUS'
Pwd_prefix.11 'GAME'
Pwd_prefix.12 'IBM'
Pwd_prefix.13 'JAN'
Pwd_prefix.14 'JUL'
Pwd_prefix.15 'JUN'
Pwd_prefix.16 'LOG'
Pwd_prefix.17 'MAR'
Pwd_prefix.18 'MAY'
Pwd_prefix.19 'NET'
Pwd_prefix.20 'NEW'
Pwd_prefix.21 'NOV'
Pwd_prefix.22 'OCT'
Pwd_prefix.23 'PASS'
Pwd_prefix.24 'ROS'
Pwd_prefix.25 'SEP'
Pwd_prefix.26 'SIGN'
Pwd_prefix.27 'SYS'
Pwd_prefix.28 'TEST'
Pwd_prefix.29 'TSO'
Pwd_prefix.30 'VALID'
Pwd_prefix.31 'VTAM'
Pwd_prefix.32 'XXX'
Pwd_prefix.33 '1234'

Note: RACF exit ICHPWX01 is coded to call a System REXX named IRRPWREX, so the name cannot be changed without a corresponding change to ICHPWX01.

System REXX requires that this exec (IRRPWREX) reside in the REXXLIB concatenation.

Update parameters in IRRPWREX according to table Parameters for RACF IRRPWREX as listed above.

CCI: CCI-000193

CCI: CCI-000194

CCI: CCI-000195

CCI: CCI-000366

CCI: CCI-001619

Group ID (Vulid): V-230210

Group Title: SRG-OS-000070-GPOS-00038

Rule ID: SV-230210r918623_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000785](#)

Rule Title: IBM RACF exit ICHPWX11 for password phrases must be installed and properly configured.

Legacy ID: V-56691

Legacy ID: SV-70951

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

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

Check Content:

From a system console screen issue the following modify command:

```
F AXR,IRRPHREX LIST
```

Review the results of the modify command.

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

-The number of required character types is 4

(assures that at least 1 upper case, 1 lower case, 1 number, and 1 special character is used in Password phrase)

-The user's name is not contained in the password phrase
(Only 3 consecutive characters of the user's name are allowed)

-The minimum password phrase length checked is 15

-The user ID is not contained in the password phrase
(Only 3 consecutive characters of the user ID are allowed)

-The new password phrase is at least 50% changed positions of the old password phrase.
(These positions need to be consecutive to cause a failure and this check is not case sensitive)

-A minimum list of 8 restricted words are being checked:
'IBM' , 'RACF', 'PASSWORD', 'PHRASE', 'PASSPHRASE', 'SECRET', 'IBMUSER', 'SYS1'

If the modify command fails or returns the following message in the system log, this is a finding.

IRX0406E REXX exec load file REXXLIB does not contain exec member IRRPHREX.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

For z/OS release 1.12 through z/OS release 2.1, APARs OA43998 and OA43999 must be applied.

Install exit IRRPHREX according to the following guidelines:
REXX Parameter Setting

```
Phr_minlen = 15 /* Minimum length */
Phr_maxlen = 100 /* Maximum passphrase length */
numbers = '0123456789'
letters = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ'
special = '&*@ :=!-%.#?|- '
Phr_allowed_chars = numbers||letters||special
Phr_leading_blanks = 'no'
Phr_trailing_blanks = 'no'
Phr_name_allowed = 'no'
Phr_name_minlen = 3
Phr_repeat_chars_chk = 'yes'
Phr_userid_allowed = 'no'
Phr_req_types = 4
Phr_min_unique = Phr_minlen % 2 /* 'Half' of chars must be unique */
Phr_min_unique_norm = 'yes'
Phr_word_unique = 0
Phr_word_unique_upper = 'yes'
Phr_word_minlen = 4
Phr_dict.1 = 'IBM'
```

Phr_dict.2 = 'RACF'
Phr_dict.3 = 'PASSWORD'
Phr_dict.4 = 'PHRASE'
Phr_dict.5 = 'PASSPHRAS
Phr_dict.6 = 'SECRET'
Phr_dict.7 = 'IBMUSER'
Phr_dict.8 = 'SYS1'

Note: RACF exit ICHPHX11 is coded to call a System REXX named IRRPHREX, so the name cannot be changed without a corresponding change to ICHPWX11.

System REXX requires that this exec (IRRPHREX) reside in the REXXLIB concatenation.

Update parameters in IRRPHREX according to table Parameters for RACF IRRPWREX as listed above.

CCI: CCI-000193

Group ID (Vulid): V-223726

Group Title: SRG-OS-000075-GPOS-00043

Rule ID: SV-223726r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000790](#)

Rule Title: The IBM RACF SETROPTS PASSWORD(MINCHANGE) value must be set to 1.

Legacy ID: SV-107263

Legacy ID: V-98159

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 the ISPF Command Shell enter:
SETRopts List

If the PASSWORD(MINCHANGE) value shows PASSWORD MINIMUM CHANGE INTERVAL IS <1> DAYS, this is not a finding.

Fix Text: Configure PASSWORD(MINCHANGE) SETROPTS value number to "1". This specifies the number of days that must pass before a user can change their password.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including PASSWORD MINCHANGE. Use the following command as an example command:
SETRPTS PASSWORD(MINCHANGE(1))

CCI: CCI-000198

Group ID (Vulid): V-223727

Group Title: SRG-OS-000076-GPOS-00044

Rule ID: SV-223727r868826_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000800](#)

Rule Title: IBM RACF SETROPTS PASSWORD(INTERVAL) must be set to 60 days.

Legacy ID: SV-107265

Legacy ID: V-98161

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. INTERVAL specifies the maximum number of days that each user's password is valid. When a user logs on to the system, RACF compares the system password interval value specified in the user profile. RACF uses the lower of the two values to determine if the users password has expired.

Check Content:

From the ISPF Command Shell enter:
SETRpts List

If the PASSWORD(INTERVAL) value is set properly and the message is PASSWORD CHANGE INTERVAL IS 060 DAYS, this is not a finding.

Fix Text: Configure PASSWORD(INTERVAL) SETROPTS value to "060" days. This specifies the maximum number of days that each user's password is valid.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including PASSWORD INTERVAL.

Setting the password interval to 60 days is activated with the command SETR PASSWORD(INTERVAL(60)).

CCI: CCI-000199

Group ID (Vulid): V-223728

Group Title: SRG-OS-000077-GPOS-00045

Rule ID: SV-223728r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000810](#)

Rule Title: The IBM RACF PASSWORD(HISTORY) SETROPTS value must be set to 5 or more.

Legacy ID: SV-107267

Legacy ID: V-98163

Vulnerability Discussion: Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. HISTORY specifies the number of previous passwords that RACF saves for each USERID and compares with an intended new password. If there is a match with one of the previous passwords, or with the current password, RACF rejects the intended new password.

Check Content:

From the ISPF Command Shell enter:

SETRopts List

If the PASSWORD(HISTORY) value is set properly then the message x GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED, where x is a minimum of "5", this is not a finding.

Fix Text: Configure the PASSWORD(HISTORY) SETROPTS value is set to a minimum of "5". This specifies the number of previous passwords that RACF saves for each USERID and compares with an intended new password. If there is a match with one of the previous passwords, or with the current password, RACF rejects the intended new password.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including PASSWORD HISTORY.

Setting the password history to 10 generations is activated with the command SETR
PASSWORD(HISTORY(10)).

CCI: CCI-000200

Group ID (Vulid): V-223729

Group Title: SRG-OS-000073-GPOS-00041

Rule ID: SV-223729r877397_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-ES-000820](#)

Rule Title: NIST FIPS-validated cryptography must be used to protect passwords in the security database.

Legacy ID: V-98165

Legacy ID: SV-107269

Vulnerability Discussion: 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.

Operating systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

Satisfies: SRG-OS-000073-GPOS-00041, SRG-OS-000074-GPOS-00042, SRG-OS-000120-GPOS-00061

Check Content:

From the ISPF Command Shell enter:

SETRopts List

If the following is specified under PASSWORD PROCESSING OPTIONS: THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS KDFAES, this is not a finding.

Fix Text: Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified below:

For z/OS release 1.12 through z/OS release 2.1 APARs OA43998 and OA43999 must be applied.

Set the passwords option for algorithm to KDFAES.

Sample syntax to activate:

SETRopts PASSWORD(ALGORITHM(KDFAES))

CCI: CCI-000196

CCI: CCI-000197

CCI: CCI-000803

Group ID (Vulid): V-223731

Group Title: SRG-OS-000138-GPOS-00069

Rule ID: SV-223731r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000840](#)

Rule Title: The IBM RACF ERASE ALL SETROPTS value must be set to ERASE(ALL) on all systems.

Legacy ID: V-98169

Legacy ID: SV-107273

Vulnerability Discussion: Preventing unauthorized information transfers mitigates the risk of information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

This requirement generally applies to the design of an information technology product, but it can also apply to the configuration of particular information system components that are, or use, such products. This can be verified by acceptance/validation processes in DoD or other government agencies.

There may be shared resources with configurable protections (e.g., files in storage) that may be assessed on specific information system components.

Check Content:

From the ISPF Command Shell enter:

SETRopts List

For all systems, if the ERASE values are set as follows, this is not a finding.

ERASE-ON-SCRATCH IS ACTIVE, CURRENT OPTIONS:
ERASE-ON-SCRATCH FOR ALL DATA SETS IS IN EFFECT

Fix Text: Configure the ERASE SETROPTS value to ERASE(ALL) this allows DASD datasets to be erased when deleted.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

-Issue the RACF Command SETR LIST to show the status of RACF Controls including the status of the ERASE options.

-Take the appropriate actions to ensure that the SETR ERASE(ALL) has been issued to enable Erase On Scratch for all datasets.

CCI: CCI-001090

Group ID (Vulid): V-223732

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223732r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-ES-000850](#)

Rule Title: IBM RACF DASD Management USERIDs must be properly controlled.

Legacy ID: V-98171

Legacy ID: SV-107275

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:

This applies to non-SMS volumes. For SMS-Managed volumes this is Not Applicable.

Ask the system administrator for all documents and procedures that apply to Storage Management, including identification of the DASD backup data sets and associated storage management userids.

From the ISPF Command enter:
RL User for each identified Userid.

Review storage management userids, if the following guidance is true, this is not a finding.

Storage management userids will not be given the "OPERATIONS" attribute.

Storage management userids will be defined with the "PROTECTED" attribute.

Storage management userids are permitted to the appropriate "STGADMIN" profiles in the "FACILITY" class for SMS-managed volumes.

Storage management userids assigned to storage management tasks (e.g., volume backup, data set archive and restore, etc.) are given access to data sets using "DASDVOL" and/or "GDASDVOL" profiles for non-SMS-managed volumes.

NOTE: "DASDVOL" profiles will not work with SMS-managed volume. "FACILITY" class profiles must be used instead. If "DFSMS/MVS" is used to perform DASD management operations, "FACILITY" class profiles may also be used to authorize storage management operations to non-SMS-managed volumes in lieu of using "DASDVOL" profiles. Therefore, not all volumes may be defined to the "DASDVOL/GDASDVOL" resource classes, and not all storage management userids may be represented in the profile access lists.

Fix Text: Note: This applies to non-SMS volumes. Refer to the System Managed Storage group (i.e., ZSMSnnnn) for requirements for System managed Storage.

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

Ensure that storage management userids do not possess the "OPERATIONS" attribute. A sample command to accomplish this is shown here:

```
ALU <userid> NOOPERATIONS
```

Ensure that storage management userids possess the "PROTECTED" attribute. A sample command to accomplish this is shown here:

```
ALU <userid> NOPASS NOOIDCARD
```

Ensure that storage management userids are permitted to the appropriate "STGADMIN" profiles in the "FACILITY" class for SMS-managed volumes.

Ensure that storage management userids are permitted to appropriate "DASDVOL" profiles for non-SMS-managed volumes.

CCI: CCI-000213

Group ID (Vulid): V-257135
Group Title: SRG-OS-000073-GPOS-00041
Rule ID: SV-257135r904403_rule
Severity: CAT II
Rule Version (STIG-ID): [RACF-ES-000860](#)
Rule Title: IBM Passtickets must be configured to be KeyEncrypted.

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

Check Content:

From the ISPF Command Shell enter:

```
RList PTKTDATA * SSIGNON NORACF
```

If any profile is not defined as KEYENCRYPTED, this is a finding.

Fix Text: Ensure that all Passticket profiles are configured to be KeyEncrypted.

CCI: CCI-000196

Group ID (Vulid): V-223733
Group Title: SRG-OS-000032-GPOS-00013
Rule ID: SV-223733r868828_rule
Severity: CAT II
Rule Version (STIG-ID): [RACF-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-98173
Legacy ID: SV-107277

Vulnerability Discussion: The FTP Server can provide audit data in the form of SMF records. The SMF data produced by the FTP Server provides transaction information for both successful and unsuccessful FTP commands. Failure to collect and retain audit data may contribute to the loss of accountability and hamper security audit activities.

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

Check Content:

If FTPDATA is configured with the following SMF statements, this is not a finding.

FTP.DATA Configuration Statements

SMF TYPE119

SMFJES TYPE119

SMFSQL TYPE119

SMFAPPE [Not coded or commented out]

SMFDEL [Not coded or commented out]

SMFEXIT [Not coded or commented out]

SMFLOGN [Not coded or commented out]

SMFREN [Not coded or commented out]

SMFRETR [Not coded or commented out]

SMFSTOR [Not coded or commented out]

Fix Text: Configure SMF options to conform to the specifications in the FTPDATA Configuration Statements below:

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-223734

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223734r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-FT-000020](#)

Rule Title: IBM RACF permission bits and user audit bits for HFS objects that are part of the FTP server component must be properly configured.

Legacy ID: V-98175

Legacy ID: SV-107279

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: With the assistance of a systems programmer with UID(0) and/or SUPERUSER access, configure the UNIX permission bits and user audit bits on the HFS directories and files for the FTP Server to conform to the specifications in the table below:

FTP Server HFS Object Security Settings
File Permission Bits User Audit Bits
/usr/sbin/ftpd 1740 fff
/usr/sbin/ftpdns 1755 fff
/usr/sbin/tftpd 0644 faf
/etc/ftp.data 0744 faf

`/etc/ftp.banner 0744 faf`

The `/usr/sbin/ftpd` and `/usr/sbin/ftpdns` objects are symbolic links to `/usr/lpp/tcpip/sbin/ftpd` and `/usr/lpp/tcpip/sbin/ftpdns` respectively. The permission and user audit bits on the targets of the symbolic links must have the required settings.

The TFTP Server does not perform any user identification or authentication, allowing any client to connect to the TFTP Server. Due to this lack of security, the TFTP Server will not be used. The TFTP Client is not secured from use.

The `/etc/ftp.data` file may not be the configuration file the server uses. It is necessary to check the `SYSFTPD DD` statement in the FTP started task JCL to determine the actual file.

The `/etc/ftp.banner` file may not be the banner file the server uses. It is necessary to check the `BANNER` statement in the FTP Data configuration file to determine the actual file.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
- no auditing

Some of the files listed above (e.g., `/etc/ftp.data`) are not used in every configuration. While the absence of a file is generally not a security issue, the existence of a file that has not been properly secured can often be an issue. Therefore, all files that do exist should have the specified permission and audit bit settings.

The following commands can be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

```
chmod 1740 /usr/lpp/tcpip/sbin/ftpd
chaudit rwx=f /usr/lpp/tcpip/sbin/ftpd
chmod 1755 /usr/lpp/tcpip/sbin/ftpdns
chaudit rwx=f /usr/lpp/tcpip/sbin/ftpdns
chmod 0744 /etc/ftp.data
```

```
chaudit w=sf,rx+f /etc/ftp.data
chmod 0744 /etc/ftp.banner
chaudit w=sf,rx+f /etc/ftp.banner
```

CCI: CCI-000213

Group ID (Vulid): V-223735

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223735r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-FT-000030](#)

Rule Title: IBM z/OS data sets for the FTP server must be properly protected.

Legacy ID: V-98177

Legacy ID: SV-107281

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:

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

If WRITE and ALLOCATE access to the data set containing the FTP Data configuration file is restricted to systems programming personnel, this is not a finding.

Note: READ access to all authenticated users is permitted.

If WRITE and ALLOCATE access to the data set containing the FTP Data configuration file is logged, this is not a finding.

If WRITE and ALLOCATE access to the data set containing the FTP banner file is restricted to systems programming personnel, this is not a finding.

Note: READ access to the data set containing the FTP banner file is permitted to all authenticated users.

Notes: The MVS data sets mentioned above are not used in every configuration. Absence of a data set will not be considered a finding. The data set containing the FTP Data configuration file is determined by checking the SYSFTPD DD statement in the FTP started task JCL. The data set containing the FTP banner file is determined by checking the BANNER statement in the FTP

Data configuration file.

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

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-223736

Group Title: SRG-OS-000023-GPOS-00006

Rule ID: SV-223736r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-FT-000040](#)

Rule Title: IBM z/OS FTP.DATA configuration statements must indicate a BANNER statement with the proper content.

Legacy ID: V-98179

Legacy ID: SV-107283

Vulnerability Discussion: Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read & consent to terms in IS user agreem't."

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007

Check Content:

Refer to the 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.

Ensure the BANNER statement in the FTP Data configuration file specifies an HFS file or data set that contains a logon banner with the Standard Mandatory DoD Notice and Consent 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.

-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.

If the BANNER statement in the FTP Data configuration file does not specify an HFS file or z/OS data set that contains the Standard Mandatory DoD Notice and Consent Banner, this is a finding.

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 Standard Mandatory DoD Notice and Consent 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-223737

Group Title: SRG-OS-000228-GPOS-00088

Rule ID: SV-223737r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-FT-000050](#)

Rule Title: IBM z/OS FTP.DATA configuration statements for the FTP server must specify the BANNER statement.

Legacy ID: SV-107285

Legacy ID: V-98181

Vulnerability Discussion: Display of a standardized and approved use notification before granting access to the publicly accessible operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read & consent to terms in IS user agreem't."

Check Content:

Refer to the 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 configuration to include the BANNER statement.

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

Group ID (Vulid): V-223739

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223739r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-FT-000070](#)

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-223740

Group Title: SRG-OS-000368-GPOS-00154

Rule ID: SV-223740r853607_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-FT-000080](#)

Rule Title: The IBM z/OS TFTP server program must be properly protected.

Legacy ID: V-98187

Legacy ID: SV-107291

Vulnerability Discussion: Control of program execution is a mechanism used to prevent execution of unauthorized programs. Some operating systems may provide a capability that runs counter to the mission or provides users with functionality that exceeds mission requirements. This includes functions and services installed at the operating system level.

Some of the programs, installed by default, may be harmful or may not be necessary to support essential organizational operations (e.g., key missions, functions). Removal of executable programs is not always possible; therefore, establishing a method of preventing program execution is critical to maintaining a secure system baseline.

Methods for complying with this requirement include restricting execution of programs in certain environments, while preventing execution in other environments; or limiting execution of certain program functionality based on organization-defined criteria (e.g., privileges, subnets, sandboxed environments, or roles).

Check Content:

From the ISPF Command Shell enter:

RL Program *

If Program resources TFTPDP and EZATD are defined to the PROGRAM resource class with a UACC(NONE), this is not a finding.

The library name where these programs are located is SYS1.TCPIP.SEZALOAD.

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

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

Define the EZATD program and its alias TFTPDP to RACF with no access granted. The following commands provide a sample of how this can be accomplished.

```
rdef program tftpd addmem('sys1.tcpip.sezaload//nopadchk) -  
data('Reference SRR PDI # IFTP0090') -  
audit(all(read)) UACC(none) owner(admin)
```

```
rdef program ezatd -  
addmem('sys1.tcpip.sezaload//nopadchk) -  
data('Reference SRR PDI # IFTP0090') -  
audit(all(read)) UACC(none) owner(admin)
```

A PROGRAM class refresh will be necessary and can be accomplished with the command:

setr when(program) refresh

CCI: CCI-001764

Group ID (Vulid): V-223741

Group Title: SRG-OS-000096-GPOS-00050

Rule ID: SV-223741r868830_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-FT-000090](#)

Rule Title: IBM z/OS user exits for the FTP server must not be used without proper approval and documentation.

Legacy ID: V-98189

Legacy ID: SV-107293

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-223742

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-223742r868833_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-FT-000100](#)

Rule Title: The IBM z/OS FTP server daemon must be defined with proper security parameters.

Legacy ID: V-98191

Legacy ID: SV-107295

Vulnerability Discussion: The FTP Server daemon requires special privileges and access to sensitive resources to provide its system services. Failure to properly define and control the FTP Server 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:

From z/OS command screen enter:

ListUser FTPD OMVS (FTPD is usual name of the FTP daemon)

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

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

-The FTPD userid is defined as a PROTECTED userid.

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

From z/OS command screen enter:

RList STARTED FTPD

If a matching entry in the STARTED resource class exists enabling the use of the standard userid and appropriate group, this is not a finding.

Fix Text: Define the FTP daemon userid and a matching entry in the STARTED resource class enabling the use of the standard userid and an appropriate group.

Define the FTPD userid as a PROTECTED userid.

Define the FTPD userid with the following z/OS UNIX attributes: UID(0), HOME directory '/', shell program /bin/sh.

Sample commands to accomplish these requirements are shown here:

Add the FTPD userid:

```
AU FTPD NAME('STC, FTP Daemon') NOPASSWORD NOOIDCARD  
DFLTGRP(STCTCPX) OWNER(STCTCPX) OMVS(UID(0) HOME('/') PROGRAM('/bin/sh'))
```

```
RDEF STARTED FTPD.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))  
STDATA(USER(=MEMBER) GROUP(STCTCPX) TRACE(YES))
```

Additional permissions may be required. See SYS1.TCPIP.SEZAINST(EZARACF) or IBM Comm Server: IP Config Guide.

CCI: CCI-000764

Group ID (Vulid): V-223743

Group Title: SRG-OS-000163-GPOS-00072

Rule ID: SV-223743r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-FT-000110](#)

Rule Title: IBM FTP.DATA configuration for the FTP server must have the INACTIVE statement properly set.

Legacy ID: V-98193

Legacy ID: SV-107297

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 configuration to include an Inactive statement with a value between 1 and 900 (seconds).

CCI: CCI-001133

Group ID (Vulid): V-223744

Group Title: SRG-OS-000163-GPOS-00072

Rule ID: SV-223744r868835_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-FT-000120](#)

Rule Title: IBM z/OS startup parameters for the FTP server must have the INACTIVE statement properly set.

Legacy ID: V-98195

Legacy ID: SV-107299

Vulnerability Discussion: 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 the FTPD started task procedure.

If the SYSTCPD and SYSFTPD DD statements specify the TCP/IP Data and FTP Data configuration files respectively, this is not a finding.

If the ANONYMOUS keyword is not coded on the PARM parameter on the EXEC statement, this is not a finding.

If the ANONYMOUS=logonid combination is not coded on the PARM parameter on the EXEC statement, this is not a finding.

If the INACTIVE keyword is not coded on the PARM parameter on the EXEC statement, this is not a finding.

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-000804

CCI: CCI-001133

Group ID (Vulid): V-255935

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-255935r881297_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-IC-000010](#)

Rule Title: IBM Integrated Crypto Service Facility (ICSF) Configuration parameters must be correctly specified.

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-255936

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-255936r881300_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-IC-000020](#)

Rule Title: IBM Integrated Crypto Service Facility (ICSF) install data sets are not properly protected.

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:

```
ad 'SYS1.CSF.**' uacc(none) owner(sys1) -  
audit(success(update) failures(read)) -  
data('Vendor DS Profile: icsf')  
pe 'SYS1.CSF.**' id(syspautd tstcaudt) acc(a)  
pe 'SYS1.CSF.**' id(icsfusrs) acc(r)
```

```
ad 'sys1.csf.scsfmod0.**' owner(sys1)  
data('apf auth icsf ds') -  
audit(success(update) failures(read)) uacc(none)
```

```
pe 'sys1.csf.scsfmod0.**' id(syspau dt tstcaudt) acc(a)
```

```
setr generic(dataset) refresh
```

CCI: CCI-000213

CCI: CCI-002264

Group ID (Vulid): V-255939

Group Title: SRG-OS-000259-GPOS-00100

Rule ID: SV-255939r881309_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-IC-000030](#)

Rule Title: IBM Integrated Crypto Service Facility (ICSF) STC data sets must be properly protected.

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 RACF data set access authorizations do not restrict READ access to auditors, this is a finding

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

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

Fix Text: Ensure that WRITE and/or greater access to IBM Integrated Crypto Service Facility (ICSF) STC and/or batch data sets are limited to system programmers and ICSF STC and/or batch jobs only. READ access can be given to auditors at the 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 confirm that they are properly restricted to the ACP (Access Control Program) active on the system.

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

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:

```
ad 'sys3.csf.**' uacc(none) owner(sys3) -  
audit(failures(read)) -  
data('ICSF Output Data')  
pe 'sys3.csf.**' id(syspautd) acc(a)  
pe 'sys3.csf.**' id(tstcaudt) acc(a)  
pe 'sys3.csf.**' id(icsfstc) acc(a)  
pe 'sys3.csf.**' id(audtaudt) acc(r)
```

CCI: CCI-001499

Group ID (Vulid): V-255937

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-255937r881303_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-IC-000040](#)

Rule Title: IBM Integrated Crypto Service Facility (ICSF) Started Task name is not properly identified / defined to the system ACP.

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 ISPF Command Shell-
enter ListUser

If the userid(s) for the IBM Integrated Crypto Service Facility (ICSF) started task is not defined to the security database, 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 ESM.

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:

```
AU CSFSTART NAME('STC, ICSF') NOPASS -  
OWNER(STC) DFLTGRP(STC) -  
DATA('START ICSF')
```

CCI: CCI-000764

Group ID (Vulid): V-255938

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-255938r881306_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-IC-000050](#)

Rule Title: IBM Integrated Crypto Service Facility (ICSF) Started task(s) must be properly defined to the STARTED resource class for RACF.

Vulnerability Discussion: Access to product resources should be restricted to only those individuals responsible for the application connectivity and who have a requirement to access these resources. Improper control of product resources could potentially compromise the operating system, ACP, and customer data.

Check Content:

Execute the RACF DSMON report for RACSPT

if the IBM Integrated Crypto Service Facility (ICSF) started task(s) is (are) not defined to the STARTED resource class profile and/or ICHRIN03 table entry this is a finding

Fix Text: Ensure that a product's started task(s) is (are) properly identified and/or defined to the System ACP.

A unique userid must be assigned for the IBM Integrated Crypto Service Facility (ICSF) started task(s) thru a corresponding STARTED class entry.

The following sample set of commands is shown here as a guideline:

```
rdef started CSFSTART.** uacc(none) owner(admin) audit(all(read)) stdata(user(CSFSTART)
group(stc))
```

```
setr racl(started) ref
```

CCI: CCI-000764

Group ID (Vulid): V-223745

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223745r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-JS-000010](#)

Rule Title: IBM z/OS RJE workstations and NJE nodes must be defined to the FACILITY resource class.

Legacy ID: V-98197

Legacy ID: SV-107301

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:

Refer to SYS1.PARMLIB (JES2PARM)

For each node entry

If all JES2 defined NJE nodes and RJE workstations have a profile defined in the FACILITY resource class, this is not a finding.

Notes: Nodename is the NAME parameter value specified on the NODE statement. Review the JES2 parameters for NJE node definitions by searching for NODE(in the report. Workstation is RMTnnnn, where nnnn is the number on the RMT statement. Review the JES2 parameters for RJE workstation definitions by searching for RMT(in the report. NJE.* and RJE.* profiles will force userid and password protection of all NJE and RJE connections respectively. This method is acceptable in lieu of using discrete profiles.

Fix Text: Configure associated PROFILEs TO exist for all RJE/NJE sources and review the authorizations for these remote facilities.

CCI: CCI-000213

Group ID (Vulid): V-223746

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223746r767087_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-JS-000020](#)

Rule Title: IBM z/OS JES2 input sources must be controlled in accordance with the proper security requirements.

Legacy ID: SV-107303

Legacy ID: V-98199

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

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

Check Content:

Refer the JES2PARM member of SYS1.PARMLIB.

Review the following resources in the RACF JESINPUT resource class:

INTRDR (internal reader for batch jobs)
nodename (NJE node)
OFFn.* (spool offload receiver)
Rnnnn (RJE workstation)
RDRnn (local card reader)
STCINRDR (internal reader for started tasks)
TSUINRDR (internal reader for TSO logons)

Note: If any of the following are not defined within the JES2 parameters, the resource in the JESINPUT resource class does not have to be defined.

- Nodename is the NAME parameter in the NODE statement. Review the NJE node definitions by searching for NODE(in the report.
- OFFn, where n is the number of the offload receiver. Review the spool offload receiver definitions by searching for OFF(in the report.
- Rnnnn, where nnnn is the number of the remote workstation. Review the RJE node definitions by searching for RMT(in the report.
- RDRnn, where nn is the number of the reader. Review the reader definitions by searching for RDR(in the report.

If the JESINPUT resource class is active, this is not a finding.

If the resources detailed above are protected by generic and/or fully qualified profiles defined to the JESINPUT resource class, this is not a finding.

Fix Text: Review the following resources in the JESINPUT resource class:

INTRDR (internal reader for batch jobs)
nodename (NJE node)
OFFn.* (spool offload receiver)
Rnnnn (RJE workstation)
RDRnn (local card reader)
STCINRDR (internal reader for started tasks)
TSUINRDR (internal reader for TSO logons)

Note: If any of the following are not defined within the JES2 parameters, the resource in the JESINPUT resource class does not have to be defined.

- Nodename is the NAME parameter in the NODE statement. Review the JES2 parameters for NJE node definitions by searching for NODE(in the report.
- OFFn, where n is the number of the offload receiver. Review the JES2 parameters for spool offload receiver definitions by searching for OFF(in the report.
- Rnnnn, where nnnn is the number of the remote workstation. Review the JES2 parameters for RJE node definitions by searching for RMT(in the report.
- RDRnn, where nn is the number of the reader. Review the JES2 parameters for reader

definitions by searching for RDR(in the report.

Define the JESINPUT resource class to the ACTIVE CLASSES in RACF SETROPTS.

Configure the resources detailed above to be protected by generic and/or fully qualified profiles defined to the JESINPUT resource class.

Examples:

```
setr classact(jesinput)
setr generic(jesinput)
rdef jesinput intrdr UACC(none) owner(admin) audit(failures(read) success(update)) data('Per
SRR PDI ZJES0021')
pe intrdr cl(jesinput) id(<syspsmpl>)
pe intrdr cl(jesinput) id(*) /* all users */
```

CCI: CCI-000213

Group ID (Vulid): V-223747

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223747r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-JS-000030](#)

Rule Title: IBM z/OS JES2 input sources must be properly controlled.

Legacy ID: SV-107305

Legacy ID: V-98201

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:

RL JESINPUT *

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

INTRDR
nodename
OFFn.*
OFFn.JR
OFFn.SR
Rnnnn.RDm
RDRnn
STCINRDR
TSUINRDR and/or TSOINRDR

Note: Examples of appropriate might be access to the offload input sources is limited to systems personnel (e.g., operations staff) as directed by site operations and the site security plan.

Fix Text: Configure access for resources defined to the JESINPUT resource class to restrict to the appropriate personnel.

Grant read access to authorized users for each of the following input sources:

INTRDR
nodename
OFFn.*
OFFn.JR
OFFn.SR
Rnnnn.RDm
RDRnn
STCINRDR
TSUINRDR and/or TSOINRDR

The resource definition will be generic if all of the resources of the same type have identical access controls (e.g., if all off load receivers are equivalent).

CCI: CCI-000213

Group ID (Vulid): V-223748

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223748r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-JS-000040](#)

Rule Title: IBM z/OS JES2 output devices must be controlled in accordance with the proper security requirements.

Legacy ID: SV-107307

Legacy ID: V-98203

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

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

Check Content:

Refer the JES2PARM member of SYS1.PARMLIB.

Review the following resources in the RACF WRITER resource class:

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)

-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.

If the WRITER resource class is active, this is not a finding.

If the other resources detailed above are protected by generic and/or fully qualified profiles defined to the WRITER resource class with UACC(NONE), this is not a finding.

Fix Text: Review the following resources in the WRITER resource class:

- 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)

- 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.

Define the WRITER resource class to the ACTIVE CLASSES in RACF SETROPTS.

Configure the profile JES2.** to have no access in the WRITER resource class.

Configure the resources detailed above to be protected by generic and/or fully qualified profiles defined to the WRITER resource class.

Examples:

```
setr classact(writer)
setr gencmd(writer) generic(writer)
setr raclist(writer)
RDEF WRITER JES2.** owner(admin) AUDIT(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.** owner(admin) AUDIT(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.OFF*.JT owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.OFF*.ST owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.PRT* owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.PUN* owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.NJE.** owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.RJE.** owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
```

```
pe JES2.** cl(writer) id(<syspsmpl>)
pe JES2.LOCAL.** cl(writer) id(<syspsmpl>)
pe JES2.LOCAL.OFF*.JT cl(writer) id(<syspsmpl>)
pe JES2.LOCAL.OFF*.ST cl(writer) id(<syspsmpl>)
pe JES2.LOCAL.PRT* cl(writer) id(<syspsmpl>)
pe JES2.LOCAL.PUN* cl(writer) id(<syspsmpl>)
pe JES2.NJE.** cl(writer) id(<syspsmpl>)
pe JES2.RJE.** cl(writer) id(<syspsmpl>)
setr racl(writer) Ref
```

CCI: CCI-000213

Group ID (Vulid): V-223749

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223749r868841_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-JS-000050](#)

Rule Title: IBM z/OS JES2 output devices must be properly controlled for classified systems.

Legacy ID: V-98205

Legacy ID: SV-107309

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:

RL WRITER *

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

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: Examples of appropriate restriction might be access to the offload input sources is limited to systems personnel (e.g., operations staff) as directed by site operations and the site security plan.

Fix Text: Configure access authorization for resources defined to the WRITER resource class to be restricted to the operators and system programmers on a classified system only.

Define resources in the ACP's respective WRITER class for each of the following output destinations:

JES2.LOCAL.devicename

JES2.LOCAL.OFFn.*
JES2.LOCAL.OFFn.JT
JES2.LOCAL.OFFn.ST
JES2.LOCAL.PRTn
JES2.LOCAL.PUNn
JES2.NJE.nodename
JES2.RJE.devicename

CCI: CCI-000213

Group ID (Vulid): V-223750

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223750r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-JS-000060](#)

Rule Title: IBM z/OS JESSPOOL resources must be protected in accordance with security requirements.

Legacy ID: V-98207

Legacy ID: SV-107311

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:

SETRopt list

If the JESSPOOL resource class is active, this is not a finding.

Fix Text: Configure the JESSPOOL resource class to be active:

Use the RACF Command: SETROPTS CLASSACT(JESSPOOL).

CCI: CCI-000213

Group ID (Vulid): V-223751

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223751r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-JS-000070](#)

Rule Title: IBM z/OS JESNEWS resources must be protected in accordance with security requirements.

Legacy ID: V-98209

Legacy ID: SV-107313

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:

RL OPERCMS *

JES2 is typically the name of the JES2 subsystem. Refer to the SUBSYS report and locate the entry with the description of PRIMARY JOB ENTRY SUBSYSTEM. The SUBSYSTEM NAME of this entry is the name of the JES2 subsystem.

If the JES2.UPDATE.JESNEWS resource is defined to the OPERCMDS resource class, this is not a finding.

If access authorization to the JES2.UPDATE.JESNEWS resource in the OPERCMDS class restricts CONTROL access to the appropriate personnel (i.e., users responsible for maintaining the JES News data set), this is not a finding.

If all access to the JES2.UPDATE.JESNEWS resource is logged, this is not a finding.

Fix Text: Refer to "Protecting JESNEWS" in Chapter 7 of the JES2 Init & Tuning Guide.

a) 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 NONE and all access is logged.

NOTE: JES2 is typically the name of the JES2 subsystem. Refer to the SUBSYS report and locate the entry with the description of PRIMARY JOB ENTRY SUBSYSTEM. The SUBSYSTEM NAME of this entry is the name of the JES2 subsystem.

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

Examples of setting up proper protection are shown here:

```
RDEF OPERCMDS JES2.UPDATE.JESNEWS UACC(NONE) OWNER(ADMIN)
AUDIT(ALL(READ)) DATA('COMPLY WITH ZJES0042')
```

```
PERMIT JES2.UPDATE.JESNEWS CLASS(OPERCMDS) ID(<syspsmpl>)
ACCESS(CONTROL)
```

CCI: CCI-000213

Group ID (Vulid): V-223752

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223752r767089_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-JS-000080](#)

Rule Title: IBM z/OS JESTRACE and/or SYSLOG resources must be protected in accordance with security requirements.

Legacy ID: V-98211

Legacy ID: SV-107315

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

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

Check Content:

Refer to the JESPARM member of SYS1.PARMLIB.

Review the JES2 parameters to determine the localnodeid by searching for OWNNODE in the NJEDEF statement, and then searching for NODE(nnnn) (where nnnn is the value specified by OWNNODE). The NAME parameter value specified on this NODE statement is the localnodeid. Another method is to issue the JES2 command \$D NODE,NAME,OWNNODE=YES to obtain the NAME of the OWNNODE.

From the ISPF Command Shell enter:

```
RL JESSPOOL *
```

Review the following resources defined to the JESSPOOL resource class:

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

NOTE: These resource profiles may be more generic as long as they pertain directly to the JESTRACE and SYSLOG data sets. For example:

```
localnodeid.JES2.*.*.*.JESTRACE  
localnodeid.+MASTER+.*.*.*.SYSLOG or  
localnodeid.+BYPASS+.*.*.*.SYSLOG
```

If Userid(s) associated with external writer(s) have complete access, this is not a finding.

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.

If Systems personnel and security administrators responsible for diagnosing JES2 and z/OS problems have complete access, this is not a finding.

If Application Development and Application Support personnel responsible for diagnosing application problems have READ access to the SYSLOG resource, this is not a finding.

Fix Text: Configure RACF access authorization for resources defined to the JESTRACE and SYSLOG resources in the JESSPOOL resource class to be restricted to the appropriate personnel a detailed below.

Review the following resources defined to the JESSPOOL resource class:

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

Note: These resource profiles may be more generic as long as they pertain directly to the JESTRACE and SYSLOG data sets. For example:

```
localnodeid.JES2.$TRCLOG.*.**  
localnodeid.+MASTER+.SYSLOG.*.** or  
localnodeid.+BYPASS+.SYSLOG.*.**
```

Note: Review the JES2 parameters to determine the localnodeid by searching for OWNNODE in the NJEDEF statement, and then searching for NODE(nnnn) (where nnnn is the value specified by OWNNODE). The NAME parameter value specified on this NODE statement is the localnodeid. Another method is to issue the JES2 command \$D NODE,NAME,OWNNODE=YES to obtain the NAME of the OWNNODE.

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

Userid(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.

Examples:

```
RDEFINE JESSPOOL localnodeid.JES2.$TRCLOG.*.** audit(failures(read)) UACC(none) -  
data('Reference srr finding ZJES0044 ') owner(admin)
```

```
RDEFINE JESSPOOL localnodeid.+MASTER+.SYSLOG.*.** audit(failures(read))  
UACC(none) -  
data('Reference srr finding ZJES0044') owner(admin)
```

or

```
RDEFINE JESSPOOL localnodeid.+BYPASS+.SYSLOG.*.** audit(failures(read))
```

UACC(none) -
data('Reference srr finding ZJES0044') owner(admin)

PE localnodeid.JES2.\$TRCLOG.** cl(jesspool) id(<syspsmpl> <secasmpl>) acc(a)
PE localnodeid.+MASTER+.SYSLOG.*.** cl(jesspool) id(<syspsmpl> <secasmpl>) acc(a)
PE localnodeid.+MASTER+.SYSLOG.*.** cl(jesspool) id(<appdpsmpl> <appssmpl>) acc(r)
or
PE localnodeid.+BYPASS+.SYSLOG.*.** cl(jesspool) id(<syspsmpl> <secasmpl>) acc(a)
PE localnodeid.+BYPASS+.SYSLOG.*.** cl(jesspool) id(<appdpsmpl> <appssmpl>) acc(r)

CCI: CCI-000213

Group ID (Vulid): V-223753

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223753r868844_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-JS-000090](#)

Rule Title: IBM z/OS JES2 spool resources must be controlled in accordance with security requirements.

Legacy ID: V-98213

Legacy ID: SV-107317

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:

RL JESSPOOL *

Review the accesses to the JESSPOOL resources.

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

Review the JESSPOOL report for resource permissions with the following naming convention. These profiles 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 RACF 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. resources are restricted to only system programmers, operators, and automated operations personnel with access of ALTER. 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. UPDATE, CONTROL, and ALTER 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 accesses for JESSPOOL resources as detailed below. The JESSPOOL may have more restrictive security at the direction of the ISSO.

The JESSPOOL resources may be fully qualified, be specified as generic, or be specified with

masking as indicated below:

localnodeid.userid.jobname.jobid.dsnumber.name

localnodeid The name of the node on which the SYSIN or SYSOUT data set currently resides.

userid The userid associated with the job. This is the userid used for validation purposes when the job runs.

jobname The name that appears in the name field of the JOB statement.

jobid The job number JES2 assigned to the job.

dsnumber The unique data set number JES2 assigned to the spool data set. A D is the first character of this qualifier.

name The name of the data set specified in the DSN= parameter of the DD statement. If the JCL did not specify DSN= on the DD statement that creates the spool data set, JES2 uses a question mark (?).

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 of ALTER. All access will be logged. (localnodeid. resource includes all generic and/or masked permissions, example: localnodeid.**, localnodeid.*, etc.)

```
RDEF JESSPOOL localnodeid.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
DATA('PROTECT JESSPOOL AT HIGH LEVEL, REF ZJES0046')
PE localnodeid.** CL(JESSPOOL) ID(syspsmpl) ACC(A)
```

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, the installation may delegate to the individual users the authority to grant access, but only with the approval of the ISSO.

```
RDEF JESSPOOL localnode.userid.jobname.jobid.dsnumber.name -
UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) -
DATA('PROTECT JESSPOOL, REF ZJES0046')
```

PE localnode.userid.jobname.jobid.dsnumber.name CL(JESSPOOL) ID(<users_or_groups>)
ACC(R)

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.

Conduct a review of 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-223754

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223754r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-JS-000100](#)

Rule Title: IBM z/OS JES2 system commands must be protected in accordance with security requirements.

Legacy ID: V-98215

Legacy ID: SV-107319

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:

RList OPERCMDS *

If the JES2.** resource is defined to the OPERCMDS class with an access of NONE and all access is logged, this is not a finding.

If access to JES2 system commands defined in the IBM z/OS JES2 Commands is restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users), as determined in the documented site Security Plan, this is not a finding.

If access to specific JES2 system commands is logged as indicated 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.

Fix Text: Extended MCS support allows the installation to control the use of JES2 system commands through the ESM. These commands are subject to various types of potential abuse. For this reason, it is necessary to place restrictions on the JES2 system commands that can be entered by particular operators.

Some commands are particularly dangerous and should only be used when less drastic options have been exhausted. Misuse of these commands can create a situation in which the only recovery is an IPL.

To control access to JES2 system commands, apply the following:
implementing security:

Define the JES2.** resource in the OPERCMDS class with an access of NONE and all access is logged.

Define the JES2 system commands as specified in the IBM z/OS JES2 Commands to be restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users), as determined in the documented site Security Plan.

Define the JES2 system commands with proper logging as determined in the documented site Security Plan.

Note: Display commands and others as deemed by the site IAW site security plan may be allowed for all users with no logging.

Build a command file based on the referenced JES2 Command Table. A sample of the commands in the command file is provided here:

```
RDEF OPERCMDS JES2.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))  
DATA('REQUIRED BY SRR PDI ZJES0052')
```

```
RDEF OPERCMDS JES2.<command>.** UACC(NONE) OWNER(ADMIN)  
AUDIT(ALL(READ)) DATA('REQUIRED BY SRR PDI ZJES0052')  
PE JES2.<command>.** CL(OPERCMDS) ID(<syspsmpl>) ACC(U)
```

```
SETR RACL(OPERCMDS) REF
```

CCI: CCI-000213

Group ID (Vulid): V-223755

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223755r853608_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-JS-000110](#)

Rule Title: IBM z/OS surrogate users must be controlled in accordance with proper security requirements.

Legacy ID: V-98217

Legacy ID: SV-107321

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

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

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000326-GPOS-00126

Check Content:

From the ISPF Command Shell enter:

RList SURROGAT *

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

For each executionuserid.SUBMIT resource defined to the SURROGAT resource class, if the following items are in true regarding surrogate controls, this is not a finding.

-All executionuserid.SUBMIT resources defined to the SURROGAT resource class specify a default access of NONE.

-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: Configure the SURROGAT as follows:

For executionuserid.SUBMIT resources defined to the SURROGAT resource class, ensure the following items are in effect regarding surrogate controls:

All executionuserid.SUBMIT resources defined to the SURROGAT resource class specify a default access of NONE.

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).

Consider the following recommendations when implementing security for Surrogate Users:

Keep the use of Surrogate Users outside of those granted to the scheduling software to a minimum number of individuals.

The simplest configuration is to only use Surrogate resource for the appropriate Scheduling task/software for production scheduling purposes as documented.

Temporary use of surrogate resource of the production batch 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 are determined by site policy.

Access authorization is restricted to the minimum number of personnel required for running production jobs. However, Surrogate 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 a Cross Authorized ACID would normally be utilized for scheduled batch production only and as such must normally be limited to the scheduling task such as CONTROLM) and not granted as a normal daily basis to individual users.

Command samples are provided to define/permit SURROGAT profiles:

```
SETR CLASSACT(SURROGAT)
SETR GENERIC(SURROGAT) GENCMD(SURROGAT)
SETR RACL(SURROGAT)
```

```
RDEF SURROGAT <batchid>.SUBMIT UACC(NONE) OWNER(ADMIN)
AUDIT(ALL(READ)) DATA('SUBMIT JOBS FOR <batchid>, REFERENCE ZJES0060')
```

```
PE <batchid>.SUBMIT CL(SURROGAT) ID(<authorized user such as CONTROLM>)
```

CCI: CCI-000213

CCI: CCI-002233

Group ID (Vulid): V-223756

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223756r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-JS-000120](#)

Rule Title: IBM z/OS RJE workstations and NJE nodes must be controlled in accordance with security requirements.

Legacy ID: SV-107323

Legacy ID: V-98219

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:

Note that this guidance addresses RJE Workstations that are "Dedicated". If an RJE workstation is dedicated, the assumption is that the RJE to host connection is hard-wired between the RJE and host. In this case the RMT definition statement will contain the keyword `LINE=` which specifies that this RJE is only connected via that one `LINE` statement.

Refer to the `JES2PARM` member of `PARMLIB`.

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

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

Review the `JES2` parameters for RJE workstation definitions by searching for `RMT(` in the report.

A `userid` of `RMTnnnn` is defined to `RACF` for each RJE workstation, where `nnnn` is the number on the `RMT` statement.

No `userid` segments (e.g., `TSO`, `CICS`, etc.) are defined.

Restricted from accessing all data sets and resources with exception of the corresponding `JESINPUT` class profile for that remote.

NOTE: Execute the `JCL` in `CNTL(IRRUT100)` using the `RACF RMTnnnn` `userid`s as `SYSIN` input. This report lists all occurrences of these `userid`s within the `RACF` database, including data set and resource access lists.

A `FACILITY`-Class profile exists in the format `RJE.RMTnnnn` where `nnn` identifies the remote number.

Fix Text: Note that this guidance addresses RJE Workstations that are "Dedicated". If an RJE workstation is dedicated, the assumption is that the RJE to host connection is hard-wired between the RJE and host. In this case the `RMT` definition statement will contain the keyword `LINE=` which specifies that this RJE is only connected via that one `LINE` statement.

Review the `JES2` parameters for RJE workstation definitions by searching for `RMT(` in the report.

Configure the RJE workstation userids to be defined as follows:

A userid of RMTnnnn is defined to RACF for each RJE workstation, where nnnn is the number on the RMT statement.

No userid segments (e.g., TSO, CICS, etc.) are defined.

Restricted from accessing all data sets and resources with exception of the corresponding JESINPUT-class profile for that remote.

Review Chapter 17 of the RACF Security Admin Guide. The following is an example that show proper implementation:

```
AG RMTGRP OWNER(ADMIN) SUPGROUP(ADMIN)
```

```
AU RMT777 NAME('RMT RJE 777') DFLTGRP(RMTGRP) OWNER(RMTGRP)  
DATA('COMPLY WITH ZJES0011') NOPASS RESTRICTED
```

```
PE RMT777 CL(JESINPUT) ID(RMT777)
```

Ensure that a FACILITY-Class profile exists in the format RJE.RMTnnnn where nnn identifies the remote number.

A command example is shown here:

```
RDEF FACILITY RJE.RMT777 UACC(NONE) OWNER(ADMIN) DATA('COMPLY WITH  
ZJES0011 FOR RJE 777')
```

CCI: CCI-000366

Group ID (Vulid): V-223757

Group Title: SRG-OS-000279-GPOS-00109

Rule ID: SV-223757r868847_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000010](#)

Rule Title: IBM z/OS must configure system wait times to protect resource availability based on site priorities.

Legacy ID: SV-107325

Legacy ID: V-98221

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 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 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 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-002361

Group ID (Vulid): V-223758

Group Title: SRG-OS-000032-GPOS-00013

Rule ID: SV-223758r868850_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000020](#)

Rule Title: The IBM z/OS BPX.SMF resource must be properly configured.

Legacy ID: SV-107327

Legacy ID: V-98223

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 RACF rules are as follows this is not a finding.

BPX.SMF.119.94 - READ allowed for users running the ssh, sftp, or scp client commands.
BPX.SMF.119.96 - READ allowed for users running the scp or sftp-server server commands.
BPX.SMF.119.97 - READ allowed for users running the scp or sftp client commands.

The following profile grants the permitted users the authority to write or test for any SMF record being recorded. Access should be permitted as follows:

BPX.SMF - READ access only when documented and justified in Site Security Plan.
Documentation should include a reason why a more specific profile is not acceptable.

Fix Text: Configure Facility resource class for BPX.SMF as follows:

BPX.SMF.119.94 - READ allowed for users running the ssh, sftp, or scp client commands.
BPX.SMF.119.96 - READ allowed for users running the scp or sftp-server server commands.
BPX.SMF.119.97 - READ allowed for users running the scp or sftp client commands.

The following profile grants the permitted users the authority to write or test for any SMF record being recorded. Access should be permitted as follows:

BPX.SMF - READ access only when documented and justified in Site Security Plan.
Documentation should include a reason why a more specific profile is not acceptable.

CCI: CCI-000067

Group ID (Vulid): V-223759

Group Title: SRG-OS-000392-GPOS-00172

Rule ID: SV-223759r853610_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000030](#)

Rule Title: IBM z/OS SMF recording options for the TN3270 Telnet Server must be properly specified.

Legacy ID: SV-107329

Legacy ID: V-98225

Vulnerability Discussion: The TN3270 Telnet Server can provide audit data in the form of SMF records. The SMF data produced provides information about individual sessions. This data includes the VTAM application, the remote and local IP addresses, and the remote and local IP port numbers. Failure to collect and retain audit data may contribute to the loss of accountability and hamper security audit activities.

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

Check Content:

Refer to the Profile configuration file specified on the PROFILE DD statement in the TCPIP started task JCL.

If the following configuration statement settings are in effect in the TCP/IP Profile configuration data set, this is not a finding.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration data set, the data set specified on this statement must be checked for the following items as well.

The TELNETPARMS SMFINIT statement is coded with the TYPE119 operand within each TELNETPARMS statement block.

The TELNETPARMS SMFTERM statement is coded with the TYPE119 operand within each TELNETPARMS statement block.

Note: The SMFINIT and SMFTERM statement can appear in both TELNETGLOBAL and TELNETPARM statement blocks. If duplicate statements appear in the TELNETGLOBALS, TELNETPARMS, Telnet uses the last valid statement that was specified.

Fix Text: 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: The SMFINIT and SMFTERM statement can appear in both TELNETGLOBAL and TELNETPARM statement blocks. If duplicate statements appear in the TELNETGLOBALS, TELNETPARMS, Telnet uses the last valid statement that was specified.

CCI: CCI-000067

CCI: CCI-002884

Group ID (Vulid): V-223760

Group Title: SRG-OS-000001-GPOS-00001

Rule ID: SV-223760r604139_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-OS-000040](#)

Rule Title: IBM RACF must be installed and active on the system.

Legacy ID: SV-107331

Legacy ID: V-98227

Vulnerability Discussion: Enterprise environments make account management for operating systems challenging and complex. A manual process for account management functions adds the risk of a potential oversight or other errors. IBM z/OS requires an external security manager to assure proper account management.

Check Content:

Refer to IEASYS00 member in SYS1.PARMLIB Concatenation. Determine proper IEFSSnxx member.

If RACF is defined in the SubSystem member, this is not a finding.

Fix Text: Refer to the IBM Security Server RACF System Programmer Guide and the IBM Security Server RACF Security Administrator guide to properly implement RACF on the system.

CCI: CCI-000015

Group ID (Vulid): V-223761

Group Title: SRG-OS-000123-GPOS-00064

Rule ID: SV-223761r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000050](#)

Rule Title: The IBM z/OS System Administrator (SA) must develop a process to disable emergency accounts after the crisis is resolved or 72 hours.

Legacy ID: V-98229

Legacy ID: SV-107333

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 documented process to disable emergency accounts.

If there is no documented process, this is a finding.

Examine the process, if it does not include procedures to disable emergency accounts after the crisis is resolved or 72 hours, this is a finding.

Fix Text: Develop a process to disable emergency accounts after the crisis is resolved or 72 hours.

CCI: CCI-001682

Group ID (Vulid): V-223762

Group Title: SRG-OS-000274-GPOS-00104

Rule ID: SV-223762r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000060](#)

Rule Title: The IBM z/OS System Administrator (SA) must develop a process to notify

appropriate personnel when accounts are created.

Legacy ID: V-98231

Legacy ID: SV-107335

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 develop a process to notify appropriate personnel when accounts are created.

CCI: CCI-001683

Group ID (Vulid): V-223763

Group Title: SRG-OS-000275-GPOS-00105

Rule ID: SV-223763r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000070](#)

Rule Title: The IBM z/OS System Administrator (SA) must develop a process to notify appropriate personnel when accounts are modified.

Legacy ID: V-98233

Legacy ID: SV-107337

Vulnerability Discussion: Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

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 develop a process to notify appropriate personnel when accounts are modified.

CCI: CCI-001684

Group ID (Vulid): V-223764

Group Title: SRG-OS-000276-GPOS-00106

Rule ID: SV-223764r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000080](#)

Rule Title: The IBM z/OS System Administrator (SA) must develop a process to notify appropriate personnel when accounts are deleted.

Legacy ID: V-98235

Legacy ID: SV-107339

Vulnerability Discussion: Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Check Content:

Ask the system Administrator for the documented process to notify appropriate personnel when accounts are deleted.

If there is no documented process, this is a finding.

Fix Text: Develop a documented develop a process to notify appropriate personnel when accounts are deleted.

CCI: CCI-001685

Group ID (Vulid): V-223765

Group Title: SRG-OS-000277-GPOS-00107

Rule ID: SV-223765r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000090](#)

Rule Title: The IBM z/OS System Administrator (SA) must develop a process to notify appropriate personnel when accounts are removed.

Legacy ID: V-98237

Legacy ID: SV-107341

Vulnerability Discussion: When operating system accounts are removed, 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 removal 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.

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 develop a process to notify appropriate personnel when accounts are removed.

CCI: CCI-001686

Group ID (Vulid): V-223766

Group Title: SRG-OS-000304-GPOS-00121

Rule ID: SV-223766r853611_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000100](#)

Rule Title: The IBM z/OS System Administrator (SA) must develop a process to notify Information System Security Officers (ISSOs) of account enabling actions.

Legacy ID: V-98239

Legacy ID: SV-107343

Vulnerability Discussion: Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to enable an existing disabled account. Sending notification of account enabling actions to the system administrator and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that operating system accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

In order to detect and respond to events that affect user accessibility and application processing, operating systems must audit account enabling actions and, as required, notify the appropriate individuals so they can investigate the event.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Check Content:

Ask the system Administrator for the documented processes to notify the Information System Security Officers (ISSOs) of account enabling actions.

If there is no documented process, this is a finding.

Fix Text: Develop a documented process to notify the Information System Security Officers (ISSOs) of account enabling actions.

CCI: CCI-002132

Group ID (Vulid): V-223767

Group Title: SRG-OS-000004-GPOS-00004

Rule ID: SV-223767r868853_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000110](#)

Rule Title: IBM z/OS required SMF data record types must be collected.

Legacy ID: SV-107345

Legacy ID: V-98241

Vulnerability Discussion: Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to create an account. Auditing account creation actions provides logging that can be used for forensic purposes.

To address access requirements, many operating systems may be integrated with enterprise level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000040-GPOS-00018, SRG-OS-000041-GPOS-00019, SRG-OS-000042-GPOS-00020, SRG-OS-000042-GPOS-00021, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091,

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-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 collect 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 collect at a minimum:

0 (00) - IPL
6 (06) - External Writer/ JES Output Writer/ Print Services Facility (PSF)
7 (07) - [SMF] Data Lost
14 (0E) - INPUT or RDBACK Data Set Activity
15 (0F) - OUTPUT, UPDAT, INOUT, or OUTIN Data Set Activity
17 (11) - Scratch Data Set Status
18 (12) - Rename Non-VSAM Data Set Status
24 (18) - JES2 Spool Offload
25 (19) - JES3 Device Allocation
26 (1A) - JES Job Purge
30 (1E) - Common Address Space Work
32 (20) - TSO/E User Work Accounting
41 (29) - DIV Objects and VLF Statistics
42 (2A) - DFSMS statistics and configuration
43 (2B) - JES Start
45 (2D) - JES Withdrawal/Stop
47 (2F) - JES SIGNON/Start Line (BSC)/LOGON
48 (30) - JES SIGNOFF/Stop Line (BSC)/LOGOFF
49 (31) - JES Integrity
52 (34) - JES2 LOGON/Start Line (SNA)
53 (35) - JES2 LOGOFF/Stop Line (SNA)
54 (36) - JES2 Integrity (SNA)
55 (37) - JES2 Network SIGNON

56 (38) - JES2 Network Integrity
57 (39) - JES2 Network SYSOUT Transmission
58 (3A) - JES2 Network SIGNOFF
60 (3C) - VSAM Volume Data Set Updated
61 (3D) - Integrated Catalog Facility Define Activity
62 (3E) - VSAM Component or Cluster Opened
64 (40) - VSAM Component or Cluster Status
65 (41) - Integrated Catalog Facility Delete Activity
66 (42) - Integrated Catalog Facility Alter Activity
80 (50) - RACF/TOP SECRET Processing
81 (51) - RACF Initialization
82 (52) - ICSF Statistics
83 (53) - RACF Audit Record For Data Sets
90 (5A) - System Status
92 (5C) except subtypes 10, 11 - OpenMVS File System Activity
102 (66) - DATABASE 2 Performance
103 (67) - IBM HTTP Server
110 (6E) - CICS/ESA Statistics
118 (76) - TCP/IP Statistics
119 (77) - TCP/IP Statistics
199 (C7) - TSOMON
230 (E6) - ACF2 or as specified in ACFFDR (vendor-supplied default is 230)
231 (E7) - TSS logs security events under this record type

CCI: CCI-000018

CCI: CCI-000130

CCI: CCI-000131

CCI: CCI-000132

CCI: CCI-000133

CCI: CCI-000134

CCI: CCI-000135

CCI: CCI-000172

CCI: CCI-001403

CCI: CCI-001404

CCI: CCI-001405

CCI: CCI-001814

CCI: CCI-002130

CCI: CCI-002234

CCI: CCI-002884

Group ID (Vulid): V-223768

Group Title: SRG-OS-000023-GPOS-00006

Rule ID: SV-223768r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000120](#)

Rule Title: IBM z/OS must employ a session manager to manage display of the Standard Mandatory DoD Notice and Consent Banner.

Legacy ID: SV-107347

Legacy ID: V-98243

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. All methods of gaining access to the system must comply with this requirement to assure that regulations are upheld.

Check Content:

Verify that any session manager in use displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the system.

If the session manager does not display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system, this is a finding.

Fix Text: Configure any session manager in use to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system.

CCI: CCI-000048

Group ID (Vulid): V-223769

Group Title: SRG-OS-000038-GPOS-00016

Rule ID: SV-223769r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000130](#)

Rule Title: IBM z/OS must specify SMF data options to assure appropriate activation.

Legacy ID: SV-107349

Legacy ID: V-98245

Vulnerability Discussion: SMF data collection is the basic unit of tracking of all system functions and actions. Included in this tracking data are the audit trails from each of the ACPs. If the control options for the recording of this tracking are not properly maintained, then accountability cannot be monitored, and its use in the execution of a contingency plan could be compromised.

Satisfies: SRG-OS-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-223770

Group Title: SRG-OS-000341-GPOS-00132

Rule ID: SV-223770r877391_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000140](#)

Rule Title: IBM z/OS SMF collection files (system MANx datasets or LOGSTREAM DASD) must have storage capacity to store at least one weeks worth of audit data.

Legacy ID: V-98247

Legacy ID: SV-107351

Vulnerability Discussion: In order to ensure operating systems have a sufficient storage capacity in which to write the audit logs, operating systems need to be able to allocate audit record storage capacity.

The task of allocating audit record storage capacity is usually performed during initial installation of the operating system.

Check Content:

Review the SMF dump procedure in there system.

If the output datasets 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-223771

Group Title: SRG-OS-000342-GPOS-00133

Rule ID: SV-223771r877390_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000150](#)

Rule Title: IBM z/OS system administrators must develop an automated process to collect and retain SMF data.

Legacy ID: V-98249

Legacy ID: SV-107353

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 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. Develop 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-223772

Group Title: SRG-OS-000343-GPOS-00134

Rule ID: SV-223772r877389_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000160](#)

Rule Title: IBM z/OS BUFUSEWARN in the SMFPRMxx must be properly set.

Legacy ID: V-98251

Legacy ID: SV-107355

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-000343-GPOS-00134, SRG-OS-000344-GPOS-00135, SRG-OS-000046-GPOS-00022

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-223773

Group Title: SRG-OS-000047-GPOS-00023

Rule ID: SV-223773r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000170](#)

Rule Title: IBM z/OS NOBUFFS in SMFPRMxx must be properly set (default is MSG).

Legacy ID: V-98253

Legacy ID: SV-107357

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:

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.

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-223774

Group Title: SRG-OS-000355-GPOS-00143

Rule ID: SV-223774r877038_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000180](#)

Rule Title: The IBM z/OS SNTP daemon (SNTPD) must be active.

Legacy ID: V-98255

Legacy ID: SV-107359

Vulnerability Discussion: Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Check Content:

From UNIX System Services ISPF Shell navigate to ribbon select tools.

Select option 1 - Work with Processes.

If SNTP Daemon (SNTPD) is not active, this is a finding.

Fix Text: Obtain a copy of this sample procedure from SEZAINST and store it in one of your PROCLIB concatenation data sets.

Perform the following step to start SNTPD as a procedure:

Invoke the procedure using the system operator start command. The following sample, SEZAINST(SNTPD), shows how to start SNTPD as a procedure:

```
/**  
/** Sample procedure for the Simple Network Time Protocol (SNTP)  
/**  
/** z/OS Communications Server Version 1 Release 13  
/** SMP/E Distribution Name: SEZAINST(EZASNPRO)  
/**  
/** Copyright: Licensed Materials - Property of IBM  
/** 5650-ZOS  
/** Copyright IBM Corp. 2002, 2015  
/**  
/** Status: CSV2R2  
/**  
/**SNTPD EXEC PGM=SNTPD,REGION=4096K,TIME=NOLIMIT,  
/**PARM='/ -d'
```

```
//SYSPRINT DD SYSOUT=*,DCB=(RECFM=F,LRECL=132,BLKSIZE=132)
//SYSIN DD DUMMY
//SYSERR DD SYSOUT=*
//SYSOUT DD SYSOUT=*,DCB=(RECFM=F,LRECL=132,BLKSIZE=132)
//CEEDUMP DD SYSOUT=*
//SYSABEND DD SYSOUT=*
```

CCI: CCI-001891

Group ID (Vulid): V-223775

Group Title: SRG-OS-000355-GPOS-00143

Rule ID: SV-223775r877038_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000190](#)

Rule Title: IBM z/OS SNTP daemon (SNTPD) permission bits must be properly configured.

Legacy ID: SV-107361

Legacy ID: V-98257

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-223776

Group Title: SRG-OS-000356-GPOS-00144

Rule ID: SV-223776r853618_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000200](#)

Rule Title: IBM z/OS PARMLIB CLOCKxx must have the Accuracy PARM properly coded.

Legacy ID: SV-107363

Legacy ID: V-98259

Vulnerability Discussion: Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network. Organizations should consider setting time periods for different types of systems (e.g., financial, legal, or mission-critical systems).

Organizations should also consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints). This requirement is related to the comparison done every 24 hours in SRG-OS-000355 because a comparison must be done in order to determine the time difference.

Check Content:

Refer to the CLOCKxx member of PARMLIB.

If the ACCURACY parm is not coded, this is a finding.

If the ACCURACY parm is coded to "1000", this is not a finding.

Fix Text: Define the CLOCKxx statement to include the ACCURACY parm set to "1000".

CCI: CCI-002046

Group ID (Vulid): V-223777

Group Title: SRG-OS-000370-GPOS-00155

Rule ID: SV-223777r853619_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-OS-000210](#)

Rule Title: IBM RACF must define UACC of NONE on all profiles.

Legacy ID: SV-107365

Legacy ID: V-98261

Vulnerability Discussion: The operating system must employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.

Check Content:

Review all Dataset and resource profiles in the RACF database.

If any are not defined with UACC NONE, this is a finding.

Fix Text: Define each dataset and resource profile with UACC(NONE)

CCI: CCI-001774

Group ID (Vulid): V-223778

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223778r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000220](#)

Rule Title: IBM z/OS PASSWORD data set and OS passwords must not be used.

Legacy ID: SV-107367

Legacy ID: V-98263

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-223780

Group Title: SRG-OS-000480-GPOS-00232

Rule ID: SV-223780r853620_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000240](#)

Rule Title: The IBM z/OS Policy Agent must employ a deny-all, allow-by-exception firewall policy for allowing connections to other systems.

Legacy ID: V-98267

Legacy ID: SV-107371

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-223781

Group Title: SRG-OS-000368-GPOS-00154

Rule ID: SV-223781r868859_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-OS-000250](#)

Rule Title: Unsupported system software must not be installed and/ or active on the system.

Legacy ID: V-98269

Legacy ID: SV-107373

Vulnerability Discussion: Control of program execution is a mechanism used to prevent execution of unauthorized programs. Some operating systems may provide a capability that runs counter to the mission or provides users with functionality that exceeds mission requirements. This includes functions and services installed at the operating system level.

Some of the programs, installed by default, may be harmful or may not be necessary to support

essential organizational operations (e.g., key missions, functions). Removal of executable programs is not always possible; therefore, establishing a method of preventing program execution is critical to maintaining a secure system baseline.

Methods for complying with this requirement include restricting execution of programs in certain environments, while preventing execution in other environments; or limiting execution of certain program functionality based on organization-defined criteria (e.g., privileges, subnets, sandboxed environments, or roles).

Check Content:

This check applies to all products that meet the following criteria:

- Uses authorized and restricted z/OS interfaces by utilizing Authorized Program Facility (APF) authorized modules or libraries.
- Requires access to system datasets or sensitive information or requires special or privileged authority to run.

For the products in the above category, refer to the Vendor's support lifecycle information for current versions and releases.

If the software products currently running on the reviewed system are at a version greater than or equal to the products listed in the vendor's Support Lifecycle information, this is not a finding.

Fix Text: For all products that meet the following criteria:

- Uses authorized and restricted z/OS interfaces by utilizing Authorized Program Facility (APF) authorized modules or libraries.
- Requires access to system datasets or sensitive information or requires special or privileged authority to run.

The ISSO will ensure that unsupported system software for the products in the above category is removed or upgraded prior to a vendor dropping support.

Authorized software that is NO longer supported is a CAT I vulnerability. The customer and site will be given six months to mitigate the risk, develop a supported solution, or obtain a formal letter approving such risk/software.

CCI: CCI-001764

Group ID (Vulid): V-223782

Group Title: SRG-OS-000368-GPOS-00154

Rule ID: SV-223782r853622_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000260](#)

Rule Title: IBM z/OS must not allow nonexistent or inaccessible LINKLIST libraries.

Legacy ID: V-98271

Legacy ID: SV-107375

Vulnerability Discussion: Control of program execution is a mechanism used to prevent execution of unauthorized programs. Some operating systems may provide a capability that runs counter to the mission or provides users with functionality that exceeds mission requirements. This includes functions and services installed at the operating system level.

Some of the programs, installed by default, may be harmful or may not be necessary to support essential organizational operations (e.g., key missions, functions). Removal of executable programs is not always possible; therefore, establishing a method of preventing program execution is critical to maintaining a secure system baseline.

Methods for complying with this requirement include restricting execution of programs in certain environments, while preventing execution in other environments; or limiting execution of certain program functionality based on organization-defined criteria (e.g., privileges, subnets, sandboxed environments, or roles).

Check Content:

From and ISPF Command line enter:

```
TSO ISRDDN LINKLIST
```

Review the list, if there are any DUMMY entries i.e., inaccessible LINKLIST libraries, this is a finding.

Fix Text: Review all entries contained in the LINKLIST for the actual existence of each library. Develop a plan of action to correct deficiencies.

The Linklist is a default set of libraries that MVS searches for a specified program. This facility is used so that a user does not have to know the library names in which utility types of programs are stored. Control over membership in the Linklist is specified within the operating system. The data set SYS1.PARMLIB(LNKLISTxx) 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 LNKLISTxx member unless absolutely required.

- The LNKLISTxx and PROGxx (LNKLIST entries) members will contain only required libraries. On a semiannual basis, Software Support should review the volume serial numbers, and should

verify them in accordance with the system catalog. Software Support will remove all nonexistent libraries. The ISSO should modify and/or delete the rules associated with these libraries.

CCI: CCI-001764

Group ID (Vulid): V-223783

Group Title: SRG-OS-000368-GPOS-00154

Rule ID: SV-223783r853623_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000270](#)

Rule Title: IBM z/OS must not allow nonexistent or inaccessible Link Pack Area (LPA) libraries.

Legacy ID: V-98273

Legacy ID: SV-107377

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 nonexistent libraries. The ISSO should modify and/or delete the rules associated with these libraries.

CCI: CCI-001764

Group ID (Vulid): V-223784

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-223784r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000280](#)

Rule Title: IBM z/OS must not have inaccessible APF libraries defined.

Legacy ID: V-98275

Legacy ID: SV-107379

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 which are no longer valid designations.

CCI: CCI-000381

Group ID (Vulid): V-223785

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-223785r868862_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000290](#)

Rule Title: IBM zOS inapplicable PPT entries must be invalidated.

Legacy ID: V-98277

Legacy ID: SV-107381

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.

Invalid or inapplicable PPT entries exist, a venue is provided for the introduction of trojan horse modules with security bypass capabilities.

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
```

Interpret the display as follows:

Examine contents at offset 8

Hex 'x2' - Bypass Password Protection

Hex 'x3' - Bypass Password Protection

Hex 'x4' - No Dataset Integrity

Hex 'x5' - No Dataset 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 Dataset 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>
```

If the return message is "Load Failed", make sure there is an entry in PARMLIB member SCHEDxx that revokes the excessive privilege.

If this is not true, this is a finding.

Fix Text: Review the PPT and define all entries associated with nonexistent or inapplicable modules as invalidated. Nullify the invalid IEFSDPPT entry by ensuring that there is a corresponding SCHED entry, which confers no special attributes.

Use the following recommendations and techniques to provide protection for the PPT:

Review the IEFSDPPT module and all programs that IBM has, by default, placed in the PPT to validate their applicability to the execution system. Refer to the IBM z/OS MVS Initialization and Tuning Reference documentation for the version and release of z/OS installed at the individual site for the actual contents of the default IEFSDPPT.

Modules for products not in use on the system will have their special privileges explicitly revoked. Do this by placing a PPT entry for each module in the SYS1.PARMLIB(SCHEDxx) member, specifying no special privileges. The PPT entry for each overridden program will be in the following format, accepting the default (unprivileged) values for the subparameters:

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-223786

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-223786r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000300](#)

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: V-98279

Legacy ID: SV-107383

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-223787

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-223787r604139_rule

Severity: CAT III

Rule Version (STIG-ID): [RACF-OS-000310](#)

Rule Title: IBM z/OS must not have duplicated sensitive utilities and/or programs existing in APF libraries.

Legacy ID: V-98281

Legacy ID: SV-107385

Vulnerability Discussion: Removal of unneeded or non-secure functions, ports, protocols, and services mitigate the risk of unauthorized connection of devices, unauthorized transfer of information, or other exploitation of these resources.

Check Content:

From an ISPF Command line enter:

TSO ISRDDN APF

An APF List results

On the command line enter:

DUPLICATES (make sure there is appropriate access; if there is not you may receive insufficient access errors)

If any of the list of Sensitive Utilities exist in the duplicate APF modules 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-223788

Group Title: SRG-OS-000396-GPOS-00176

Rule ID: SV-223788r877380_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000320](#)

Rule Title: The IBM z/OS systems requiring data-at-rest protection must properly employ IBM DS8880 or equivalent hardware solutions for full disk encryption.

Legacy ID: SV-107387

Legacy ID: V-98283

Vulnerability Discussion: This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. Operating systems handling data requiring "data at rest" protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.

Selection of a cryptographic mechanism is based on the need to protect the integrity of organizational information. The strength of the mechanism is commensurate with the security category and/or classification of the information. Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).

Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Satisfies: SRG-OS-000185-GPOS-00079, SRG-OS-000405-GPOS-00184, SRG-OS-000404-GPOS-00183, SRG-OS-000396-GPOS-00176

Check Content:

Determine if IBM's DS8880 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-002420

CCI: CCI-002445

CCI: CCI-002446

Group ID (Vulid): V-251107

Group Title: SRG-OS-000138-GPOS-00069

Rule ID: SV-251107r804052_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000350](#)

Rule Title: IBM z/OS sensitive and critical system data sets must not exist on shared DASDs.

Legacy ID: V-98289

Legacy ID: SV-107393

Vulnerability Discussion: Preventing unauthorized information transfers mitigates the risk of information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

This requirement generally applies to the design of an information technology product, but it can also apply to the configuration of particular information system components that are, or use, such products. This can be verified by acceptance/validation processes in DoD or other government agencies.

There may be shared resources with configurable protections (e.g., files in storage) that may be assessed on specific information system components.

Check Content:

Check HMC, VM, and z/OS on how to validate and determine a DASD volume(s) is shared.

Note: In VM issue the command "QUEUE DASD SYSTEM" this display will show shared volume(s) and indicates the number of systems sharing the volume.

Validate all machines that require access to these shared volume(s) have the volume(s) mounted.

Obtain a map or list VTOC of the shared volume(s).

Check if shared volume(s) contain any critical or sensitive data sets.

Identify shared and critical or sensitive data sets on the system being audited. These data sets can be APF, LINKLIST, LPA, Catalogs, etc, as well as product data sets.

If all of the critical or sensitive data sets identified on shared volume(s) are protected and justified to be on shared volume(s), this is not a finding.

List critical or sensitive data sets are possible security breaches, if not justified and not protected on systems having access to the data set(s) and on shared volume(s).

Fix Text: Configure all identified volumes of shared DASD to be valid within the following.

HMC
VM
z/OS

If the shared volume(s) are valid and systems having access to these shared volume(s) are valid, map disk/VTOC list to obtain data sets on the shared volume(s). From this list obtain a list of sensitive and critical system data sets that are found on the shared volume(s). Ensure that the data sets are justified to be shared on the system and to reside on the shared volume(s).

The ISSO will review all access requirements to validate that sensitive and critical system data sets are protected from unauthorized access across all systems that have access to the shared volume(s), protecting the data set(s) whether the data set(s) are used or not used on the systems that have the shared volume(s) available to them.

CCI: CCI-001090

Group ID (Vulid): V-223792

Group Title: SRG-OS-000420-GPOS-00186

Rule ID: SV-223792r853625_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000360](#)

Rule Title: The IBM z/OS Policy Agent must contain a policy that protects against or limits the effects of denial-of-service (DoS) attacks by ensuring the operating system is implementing rate-limiting measures on impacted network interfaces.

Legacy ID: V-98291

Legacy ID: SV-107395

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 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-223793

Group Title: SRG-OS-000142-GPOS-00071

Rule ID: SV-223793r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000370](#)

Rule Title: The IBM z/OS Policy Agent must contain a policy that manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service (DoS) attacks.

Legacy ID: V-98293

Legacy ID: SV-107397

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-223794

Group Title: SRG-OS-000031-GPOS-00012

Rule ID: SV-223794r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000400](#)

Rule Title: The IBM z/OS must employ a session manager that conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Legacy ID: V-98295

Legacy ID: SV-107399

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 configure 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-223795

Group Title: SRG-OS-000029-GPOS-00010

Rule ID: SV-223795r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000410](#)

Rule Title: IBM z/OS must employ a session manager to manage session lock after a 15-minute period of inactivity.

Legacy ID: V-98297

Legacy ID: SV-107401

Vulnerability Discussion: A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

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-223796

Group Title: SRG-OS-000030-GPOS-00011

Rule ID: SV-223796r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000420](#)

Rule Title: IBM z/OS must employ a session for users to directly initiate a session lock for all connection types.

Legacy ID: SV-107403

Legacy ID: V-98299

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: Develop a procedure to offload SMF files to a different system or media than the system being audited.

CCI: CCI-000058

Group ID (Vulid): V-223797

Group Title: SRG-OS-000028-GPOS-00009

Rule ID: SV-223797r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000430](#)

Rule Title: IBM z/OS must employ a session manager to manage retaining a users session lock until that user reestablishes access using established identification and authentication procedures.

Legacy ID: SV-107405

Legacy ID: V-98301

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-223798

Group Title: SRG-OS-000002-GPOS-00002

Rule ID: SV-223798r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000440](#)

Rule Title: IBM z/OS system administrator must develop a procedure to remove or disable temporary user accounts after 72 hours.

Legacy ID: SV-107407

Legacy ID: V-98303

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 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-223799

Group Title: SRG-OS-000123-GPOS-00064

Rule ID: SV-223799r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000450](#)

Rule Title: IBM z/OS system administrator must develop a procedure to remove or disable emergency accounts after the crisis is resolved or 72 hours.

Legacy ID: SV-107409

Legacy ID: V-98305

Vulnerability Discussion: IBM z/OS system administrator must develop a procedure to remove or disable emergency accounts after the crisis is resolved or 72 hours.

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-223800

Group Title: SRG-OS-000363-GPOS-00150

Rule ID: SV-223800r853626_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000460](#)

Rule Title: IBM z/OS system administrator must develop a procedure to notify designated personnel if baseline configurations are changed in an unauthorized manner.

Legacy ID: SV-107411

Legacy ID: V-98307

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-223801

Group Title: SRG-OS-000122-GPOS-00063

Rule ID: SV-223801r853627_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000470](#)

Rule Title: IBM z/OS system administrator must develop a procedure to provide an audit reduction capability that supports on-demand reporting requirements.

Legacy ID: V-98309

Legacy ID: SV-107413

Vulnerability Discussion: The ability to generate on-demand reports, including after the audit

data has been subjected to audit reduction, greatly facilitates the organization's ability to generate incident reports as needed to better handle larger-scale or more complex security incidents.

Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. The report generation capability provided by the application must support on-demand (i.e., customizable, ad hoc, and as-needed) reports.

Check Content:

Ask the system administrator for the procedure to provide an audit reduction capability that supports on-demand reporting requirements.

If there is no procedure, this is a finding.

Fix Text: Develop a procedure to provide an audit reduction capability that supports on-demand reporting requirements.

CCI: CCI-001876

Group ID (Vulid): V-223802

Group Title: SRG-OS-000126-GPOS-00066

Rule ID: SV-223802r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000480](#)

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-98311

Legacy ID: SV-107415

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-223803

Group Title: SRG-OS-000437-GPOS-00194

Rule ID: SV-223803r853628_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000490](#)

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-98313

Legacy ID: SV-107417

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-223804

Group Title: SRG-OS-000447-GPOS-00201

Rule ID: SV-223804r853629_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000500](#)

Rule Title: IBM z/OS must 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-98315

Legacy ID: SV-107419

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-223805

Group Title: SRG-OS-000479-GPOS-00224

Rule ID: SV-223805r853630_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-OS-000510](#)

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: V-98317

Legacy ID: SV-107421

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-223806

Group Title: SRG-OS-000032-GPOS-00013

Rule ID: SV-223806r853631_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-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: V-98319

Legacy ID: SV-107423

Vulnerability Discussion: SMF data collection is the basic unit of tracking of all system functions and actions. Included in this tracking data are the audit trails from each of the ACPs. If the control options for the recording of this tracking are not properly maintained, then accountability cannot be monitored, and its use in the execution of a contingency plan could be compromised.

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

Check Content:

Locate the SSH daemon configuration file, which may be found in /etc/ssh/ directory.

Alternately:

From UNIX System Services ISPF Shell navigate to ribbon select tools.

Select option 1 - Work with Processes.

If SSH Daemon is not active, this is not a finding.

Examine SSH daemon configuration file.

If ServerSMF is not coded with ServerSMF TYPE119_U83 or is commented out, this is a finding.

Fix Text: Configure the SERVERSMF statement in the SSH Daemon configuration file to TYPE119_U83.

CCI: CCI-000067

CCI: CCI-002884

Group ID (Vulid): V-223807

Group Title: SRG-OS-000033-GPOS-00014

Rule ID: SV-223807r877398_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-SH-000020](#)

Rule Title: The IBM RACF SSH daemon must be configured to use a FIPS 140-2 compliant cryptographic algorithm to protect confidential information and remote access sessions.

Legacy ID: V-98321

Legacy ID: SV-107425

Vulnerability Discussion: Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. Cryptographic modules must adhere to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Remote access (e.g., RDP) 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.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

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-001453

Group ID (Vulid): V-223809

Group Title: SRG-OS-000228-GPOS-00088

Rule ID: SV-223809r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-SH-000040](#)

Rule Title: The SSH daemon must be configured with the Standard Mandatory DoD Notice and Consent Banner.

Legacy ID: SV-107429

Legacy ID: V-98325

Vulnerability Discussion: Display of a standardized and approved use notification before granting access to the publicly accessible operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work

product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read & consent to terms in IS user agreem't."

Check Content:

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 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 below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer.

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

Group ID (Vulid): V-223810

Group Title: SRG-OS-000096-GPOS-00050

Rule ID: SV-223810r604139_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-SH-000050](#)

Rule Title: IBM z/OS SSH daemon must be configured to only use the SSHv2 protocol.

Legacy ID: SV-107431

Legacy ID: V-98327

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-223811

Group Title: SRG-OS-000068-GPOS-00036

Rule ID: SV-223811r816951_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-SH-000060](#)

Rule Title: IBM z/OS, for PKI-based authentication, must use the ICSF or ESM for key management.

Legacy ID: SV-107433

Legacy ID: V-98329

Vulnerability Discussion: Without mapping the certificate used to authenticate to the user account, the ability to determine the identity of the individual user or group will not be available for forensic analysis.

Check Content:

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

From the ISPF Command Shell enter:

OMVS

enter

find / -name *.kdb

and

find / -name *.jks

If any files are present, this is a finding.

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

Remove all .kdb and .jks key files.

CCI: CCI-000187

Group ID (Vulid): V-223812

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223812r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-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 properly configured.

Legacy ID: V-98331

Legacy ID: SV-107435

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: Configure the UNIX permission bits and user audit bits on the HFS directories and files for the Syslog daemon to conform to the specifications in the SYSLOG Daemon HFS Object Security Settings table below.

Log files should have security that prevents anyone except the syslogd process and authorized maintenance jobs from writing to or deleting them.

A maintenance process to periodically clear the log files is essential. Logging stops if the target file system becomes full.

SYSLOG Daemon HFS Object Security Settings

File Permission Bits User Audit Bits

```
/usr/sbin/syslogd 1740 fff
```

```
[Configuration File]
```

```
/etc/syslog.conf 0744 faf
```

```
[Output log file defined in the configuration file]
```

```
0744 fff
```

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
- no auditing

NOTES:

The /usr/sbin/syslogd object is a symbolic link to /usr/lpp/tcpip/sbin/syslogd. The permission and user audit bits on the target of the symbolic link must have the required settings.

The /etc/syslog.conf file may not be the configuration file the daemon uses. It is necessary to check the script or JCL used to start the daemon to determine the actual configuration file. For example, in /etc/rc:

```
_BPX_JOBNAME='SYSLOGD' /usr/sbin/syslogd -f /etc/syslog.conf
```

For example, in the SYSLOGD started task JCL:

```
//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT  
// PARM='POSIX(ON) ALL31(ON)/ -f /etc/syslogd.conf'
```

```
//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT  
// PARM='POSIX(ON) ALL31(ON) /-f //"'SYS1.TCPPARMS(SYSLOG)'"'
```

The following commands can be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

```
chmod 1740 /usr/lpp/tcpip/sbin/syslogd  
chaudit rwx=f /usr/lpp/tcpip/sbin/syslogd  
chmod 0744 /etc/syslog.conf  
chaudit w=sf,rx+f /etc/syslog.conf  
chmod 0744 /log_dir/log_file  
chaudit rwx=f /log_dir/log_file
```


CCI: CCI-000213

Group ID (Vulid): V-223813

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-223813r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-SL-000020](#)

Rule Title: The IBM z/OS Syslog daemon must be started at z/OS initialization.

Legacy ID: V-98333

Legacy ID: SV-107437

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

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

- 1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and
- 2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:

SYSLOGD may be started from the shell, a cataloged procedure (STC), or the BPXBATCH program. Additionally, other mechanisms (e.g., a job scheduler) may be used to automatically start the Syslog daemon. To thoroughly analyze this requirement you may need to view the OS SYSLOG using SDSF, find the last IPL, and look for the initialization of SYSLOGD.

If the Syslog daemon SYSLOGD is started automatically during the initialization of the z/S/ system, this is not a finding.

Fix Text: Review the files used to initialize tasks during system IPL (e.g., /etc/rc, SYS1.PARMLIB, any job scheduler definitions) configure the Syslog daemon to start automatically during z/OS system initialization.

It is important that syslogd be started during the initialization phase of the z/OS system to ensure that significant messages are not lost. As with other z/OS UNIX daemons, there is more than one way to start SYSLOGD. It can be started as a process in the /etc/rc file or as a z/OS started task.

CCI: CCI-000764

Group ID (Vulid): V-223814

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-223814r868865_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-SL-000030](#)

Rule Title: The IBM z/OS Syslog daemon must be properly defined and secured.

Legacy ID: V-98335

Legacy ID: SV-107439

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:

From z/OS command screen enter:

ListUser SYSLOGD OMVS (SYSLOGD is usual name of the SYSLOG daemon)

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

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

-The SYSLOGD userid is defined as a PROTECTED userid.

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

From z/OS command screen enter:

RList STARTED SYSLOGD

If a matching entry in the STARTED resource class exists enabling the use of the standard userid and appropriate group, this is not a finding.

Fix Text: The Syslog daemon userid is SYSLOGD.

Define the SYSLOGD userid as a PROTECTED userid.

Define the SYSLOGD userid has UID(0), HOME('/'), and PROGRAM('/bin/sh') specified in the OMVS segment.

To set up and use as an MVS Started Proc, the following sample commands are provided:

```
AU SYSLOGD NAME('stc, tcpip') NOPASSWORD NOIDCARD DFLTGRP(STC) -  
OWNER(STC) DATA('Reference ISLG0020 for proper setup ' )  
ALU SYSLOGD DFLTGRP(stctcp) )  
ALU SYSLOGD OMVS(UID(0) HOME('/') PROGRAM('/bin/sh'))  
CO SYSLOGD GROUP(stctcp) OWNER(stctcp)
```

A matching entry mapping the SYSLOGD started proc to the SYSLOGD userid is in the STARTED resource class.

```
RDEF STARTED SYSLOGD.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))  
STDATA(USER(SYSLOGD) GROUP(STC))
```

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-223815

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223815r868868_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-SM-000010](#)

Rule Title: IBM z/OS DFSMS Program Resources must be properly defined and protected.

Legacy ID: V-98337

Legacy ID: SV-107441

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 DFSMSShsm

If the installation moves these modules to another load library, the installation-defined load library must be used in the program protection.

If the RACF resources are defined with a default access of NONE, this is not a finding.

If the RACF 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 and access requirements for SMS Program Resources. Ensure the guidelines for the resource type, resources, and/or generic equivalent are specified.

The RACF resources as designated in the table above are defined with a default access of NONE.

The RACF resource access authorizations restrict access to the appropriate personnel as

designated in the table above.

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

```
RDEF PROGRAM ACBFUTO2 ADDMEM('SYS1.DSF.DGTLLIB//NOPADCHK) -  
DATA('ADDED PER SRR PDI ZSMS0012 ') -  
AUDIT(FAILURE(READ)) UACC(NONE) OWNER(ADMIN)  
PERMIT ACBFUTO2 CLASS(PROGRAM) ID(*****)
```

CCI: CCI-000213

Group ID (Vulid): V-223816

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223816r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-SM-000020](#)

Rule Title: IBM z/OS DFSMS control data sets must be protected in accordance with security requirements.

Legacy ID: V-98339

Legacy ID: SV-107443

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 RACF data set rules for the SCDS, ACDS, COMMDS, and ACS data sets restrict WRITE or greater access to only systems programming personnel, this is not a finding.

If the RACF data set rules for the SCDS, ACDS, COMMDS, and ACS data sets do not restrict WRITE or greater 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 datasets.

Fix Text: Review the SYS1.PARMLIB(IGDSMS00) 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

Configure the RACF data set rules for the SCDS, ACDS, COMMDS, and ACS data sets to restrict WRITE or greater access to only z/OS systems programming personnel.

Note: At the discretion of the ISSM, DASD administrators are allowed UPDATE access to the control datasets.

Some example commands to implement the proper controls are shown here:

```
AD 'sys3.dfsms.mmd.commnds.**' UACC(NONE) OWNER(SYS3) AUDIT(ALL(READ))  
DATA('PROTECTED PER ZSMS0020')
```

```
PE 'sys3.dfsms.mmd.commnds.**' ID(<syspsmpl>) ACC(A)
```

CCI: CCI-000213

Group ID (Vulid): V-223817
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-223817r604139_rule
Severity: CAT II

Rule Version (STIG-ID): [RACF-SM-000030](#)

Rule Title: IBM z/OS DFSMS-related RACF classes must be active.

Legacy ID: V-98341

Legacy ID: SV-107445

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

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

Check Content:

From an ISPF Command Shell enter:

SETRopts list

If ACTIVE CLASSES lists the MGMTCLAS, STORCLAS, PROGRAM, and FACILITY resources classes, this is not a finding.

Fix Text: Configure SETROpts to include MGMTCLAS, STORCLAS, PROGRAM, and FACILITY resources classes as ACTIVE.

The classes can be activated with the command:

```
SETR CLASSACT(MGMTCLAS STORCLAS PROGRAM FACILITY)
```

The classes can be RACLISTED with the command:

```
SETR RACL(MGMTCLAS STORCLAS)
```

CCI: CCI-000213

Group ID (Vulid): V-223818

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223818r868871_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-SM-000040](#)

Rule Title: IBM z/OS DFSMS resources must be protected in accordance with the proper security requirements.

Legacy ID: V-98343

Legacy ID: SV-107447

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

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

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

Check Content:

If all SMS resources and/or generic equivalent are properly protected according to the requirements specified and the following guidance is true, this is not a finding.

The STGADMIN.** profile in the FACILITY resource class has a default access of NONE and no access is granted at this level.

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 NONE.

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 = NONE.

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

Below is listed the access requirements for SMS Resources. Configure the resources and/or generic equivalent are followed.

The RACF resources are defined with a default access of NONE.

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

Ensure that no access is given to the high-level STGADMIN resource.

Example:

```
RDEF FACILITY STGADMIN.** OWNER(ADMIN) -  
UACC(NONE) AUDIT(ALL(READ))
```

Ensure no access is given to resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE.*

Example:

```
RDEF FACILITY STGADMIN.IGG.CATALOG.SECURITY.CHANGE OWNER(ADMIN) -  
UACC(NONE) AUDIT(ALL(READ))
```

The STGADMIN.DPDSRN.olddsname is restricted to system programmers and all access is logged.

Example:

```
RDEF FACILITY STGADMIN.DPDSRN.olddsname OWNER(ADMIN) -  
UACC(NONE) AUDIT(ALL(READ))
```

```
PE STGADMIN.DPDSRN.olddsname CL(FACILITY) ID(syspsmpl)
```

The STGADMIN.IGD.ACTIVATE.CONFIGURATION is restricted to system programmers and all access is logged.

Example:

```
RDEF FACILITY STGADMIN.IGD.ACTIVATE.CONFIGURATION OWNER(ADMIN) -  
UACC(NONE) AUDIT(ALL(READ))
```

```
PE STGADMIN.IGD.ACTIVATE.CONFIGURATION CL(FACILITY) ID(syspsmpl)
```

The STGADMIN.IGG.DEFDEL.UALIAS is restricted to System Programmers and Security

personnel and all access is logged.

Example:

```
RDEF FACILITY STGADMIN.IGG.DEFDEL.UALIAS OWNER(ADMIN) -  
UACC(NONE) AUDIT(ALL(READ))
```

```
PE STGADMIN.IGG.DEFDEL.UALIAS CL(FACILITY) ID(secasmpl)  
PE STGADMIN.IGG.DEFDEL.UALIAS CL(FACILITY) ID(secdsmpl)  
PE STGADMIN.IGG.DEFDEL.UALIAS CL(FACILITY) ID(syspsmpl)
```

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:

```
RDEF FACILITY STGADMIN.ADR.COPY.CNCURRNT.** OWNER(ADMIN) -  
UACC(NONE) AUDIT(FAILURE(READ))
```

```
PE STGADMIN.ADR.COPY.CNCURRNT.** CL(FACILITY) ID(endusers)
```

The following resource is restricted to Application Production Support Team members, Automated Operations, DASD managers, and system programmers.

```
STGADMIN.IDC.DCOLLECT
```

Example:

```
RDEF FACILITY STGADMIN.IDC.DCOLLECT.** OWNER(ADMIN) -  
UACC(NONE) AUDIT(FAILURE(READ))
```

```
PE STGADMIN.IDC.DCOLLECT.** CL(FACILITY) ID(appssmpl)  
PE STGADMIN.IDC.DCOLLECT.** CL(FACILITY) ID(autosmpl)  
PE STGADMIN.IDC.DCOLLECT.** CL(FACILITY) ID(dasbsmpl)  
PE STGADMIN.IDC.DCOLLECT.** CL(FACILITY) ID(dasdsmpl)  
PE STGADMIN.IDC.DCOLLECT.** CL(FACILITY) ID(syspsmpl)
```

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:

RDEF FACILITY STGADMIN.ARC.CANCEL.** OWNER(ADMIN) -
UACC(NONE) AUDIT(FAILURE(READ))

PE STGADMIN.ARC.CANCEL.** CL(FACILITY) ID(appssmpl)
PE STGADMIN.ARC.CANCEL.** CL(FACILITY) ID(dasbsmpl)
PE STGADMIN.ARC.CANCEL.** CL(FACILITY) ID(dasdsmpl)
PE STGADMIN.ARC.CANCEL.** CL(FACILITY) ID(syspsmpl)

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:

RDEF FACILITY STGADMIN.ADR.** OWNER(ADMIN) -
UACC(NONE) AUDIT(FAILURE(READ))

PE STGADMIN.ADR.** CL(FACILITY) ID(dasbsmpl)
PE STGADMIN.ADR.** CL(FACILITY) ID(dasdsmpl)
PE STGADMIN.ADR.** CL(FACILITY) ID(syspsmpl)

The following Storage Administrator functions prefix is restricted to DASD managers and system programmers and all access is logged.

STGADMIN.ADR.STGADMIN.*

Example:

RDEF FACILITY STGADMIN.ADR.STGADMIN.** OWNER(ADMIN) -
UACC(NONE) AUDIT(ALL(READ))

PE STGADMIN.ADR.STGADMIN.** CL(FACILITY) ID(dasbsmpl)
PE STGADMIN.ADR.STGADMIN.** CL(FACILITY) ID(dasdsmpl)
PE STGADMIN.ADR.STGADMIN.** CL(FACILITY) ID(syspsmpl)

CCI: CCI-000213

CCI: CCI-002235

Group ID (Vulid): V-223819

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223819r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-SM-000050](#)

Rule Title: IBM z/OS using DFSMS must properly specify SYS(x).PARMLIB(IGDSMSxx), SMS parameter settings.

Legacy ID: SV-107449

Legacy ID: V-98345

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-223820

Group Title: SRG-OS-000032-GPOS-00013

Rule ID: SV-223820r868873_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-TC-000010](#)

Rule Title: IBM z/OS PROFILE.TCPIP configuration statements for the TCP/IP stack must be coded properly.

Legacy ID: SV-107451

Legacy ID: V-98347

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.

If the following items are in effect for the configuration statements specified in the TCP/IP Profile configuration file, this is not a finding.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set

specified on this statement must be checked for the following items as well.

The SMFPARMS statement is not coded or commented out.

The DELETE statement is not coded or commented out for production systems.

The SMFCONFIG statement is coded with (at least) the FTPCLIENT and TN3270CLIENT operands.

The TCPCONFIG and UDPCONFIG statements are coded with (at least) the RESTRICTLOWPORTS operand.

If the TCPCONFIG does not have the TTLS statement coded, this is a finding.

NOTE: If the INCLUDE statement is coded, the data set specified will be checked for access authorization compliance.

Fix Text: Ensure the following items are in effect for the configuration statements specified in the TCP/IP Profile configuration file:

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

The SMFPARMS statement is not coded or commented out.

The DELETE statement is not coded or commented out for production systems.

The SMFCONFIG statement is coded with (at least) the FTPCLIENT and TN3270CLIENT operands.

The TCPCONFIG and UDPCONFIG statements are coded with (at least) the RESTRICTLOWPORTS operand.

NOTE: If the INCLUDE statement is coded, the data set specified will be checked for access authorization compliance in STIG ID ITCP0070.

BASE TCP/IP PROFILE.TCPIP CONFIGURATION STATEMENTS FUNCTIONS

INCLUDE- Specifies the name of an MVS data set that contains additional PROFILE.TCPIP statements to be used

- Alters the configuration specified by previous statements

SMFPARMS- Specifies SMF logging options for some TCP applications; replaced by SMFCONFIG

- Controls collection of audit data

DELETE- Specifies some previous statements, including PORT and PORTRANGE, that are to be deleted

- Alters the configuration specified by previous statements

SMFCONFIG- - Specifies SMF logging options for Telnet, FTP, TCP, API, and stack activity

- Controls collection of audit data

TCPCONFIG- Specifies various settings for the TCP protocol layer of TCP/IP
- Controls port access

TCPCONFIG coded with TTLS - Specifies that the AT-TLS function is activated for the TCP/IP stack. The AT-TLS function provides invocation of System SSL in the TCP transport layer of the stack.

Note: If AT-TLS is enabled, users 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-223821

Group Title: SRG-OS-000297-GPOS-00115

Rule ID: SV-223821r853633_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-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: SV-107453

Legacy ID: V-98349

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 TCP/IP PROFILE DD statement to determine the TCP/IP Ports. If the PROFILE DD

statement is not supplied, use the default search order to find the PROFILE data set.

See the IP Configuration Guide for a description of the search order for PROFILE.TCPIP.

If the all the Ports included in 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-223822

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223822r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-TC-000030](#)

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 properly configured.

Legacy ID: V-98351

Legacy ID: SV-107455

Vulnerability Discussion: HFS directories and files of the Base TCP/IP component provide the configuration, operational, and executable properties of IBM's TCP/IP system product. Failure to properly secure these objects may lead to unauthorized access resulting in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

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-223823

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223823r868876_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-TC-000040](#)

Rule Title: IBM z/OS TCP/IP resources must be properly protected.

Legacy ID: V-98353

Legacy ID: SV-107457

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:

```
RLIST SERVAUTH * ALL
```

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

The EZA, EZB, and IST resources and/or generic equivalent are defined to the SERVAUTH resource class with a UACC(NONE).

No access is given to the EZA, EZB, and IST high level resources of the SERVAUTH resource class.

If the product CSSMTP is on the system, no access is given to EZB.CSSMTP of the SERVAUTH resource class.

If the product CSSMTP is on the system, EZB.CSSMTP.sysname.writername.JESnode will be specified and made available to the CSSMTP started task and authenticated users that require access to use CSSMTP for 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.

The EZB.STACKACCESS. resource access authorizations restrict access to those started tasks

with valid requirements and users with valid FTP access requirements.

The EZB.FTP.*.*.ACCESS.HFS) resource access authorizations restrict access to FTP users with specific written documentation showing a valid requirement exists to access OMVS files and Directories.

The EZB.INITSTACK.sysname.tcpname resource access authorizations restrict access before policies have been installed, to users authorized by the system security plan requiring access to the TCP/IP stack.

Fix Text: Develop a plan of action to implement the required changes. Ensure the following items are in effect for TCP/IP resources.

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

Ensure that the EZA, EZB, and IST resources and/or generic equivalent are defined to the SERVAUTH resource class with a UACC(NONE).

No access is given to the EZA, EZB, and IST resources of the SERVAUTH resource class.

If the product CSSMTP is on the system, no access is given to EZB.CSSMTP of the SERVAUTH resource class. EZB.CSSMTP.sysname.writernode.JESnode will be specified and made available to the CSSMTP started task and authenticated users that require access to use CSSMTP for e-mail services.

Only authenticated users that require access are permitted access to the second level of the resources in the SERVAUTH resource class. Examples are the network (NETACCESS), port (PORTACCESS), stack (STACKACCESS), and FTP resources in the SERVAUTH resource class.

The EZB.STACKACCESS. resource access authorizations restrict access to those started tasks with valid requirements and users with valid FTP access requirements.

The EZB.FTP.*.*.ACCESS.HFS) resource access authorizations restrict access to FTP users with specific written documentation showing a valid requirement exists to access OMVS files and Directories.

The EZB.INITSTACK.sysname.tcpname resource access authorizations restrict access to TCP/IP stack before policies have been installed to users authorized by the system security plan.

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

```
RDEF SERVAUTH EZB.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
```

RDEF SERVAUTH EZB.CSSMTP.** UACC(NONE) OWNER(ADMIN)
AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.CSSMTP.sysname.writername.JESnode UACC(NONE)
OWNER(ADMIN) AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.FTP.** UACC(NONE) OWNER(ADMIN)
AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.NETACCESS.** UACC(NONE) OWNER(ADMIN)
AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.PORTACCESS.** UACC(NONE) OWNER(ADMIN)
AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.STACKACCESS.** UACC(NONE) OWNER(ADMIN)
AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.INITSTACK.** UACC(NONE) OWNER(ADMIN)
AUDIT(FAILURE(READ))

PE EZB.CSSMTP.sysname.writername.JESnode CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.FTP.** CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.FTP.sysname.ftpstc.ACCESS.HFS CL(SERVAUTH) ID(ftpprofile) ACC(READ)
PE EZB.NETACCESS.** CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.PORTACCESS.** CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.STACKACCESS.** CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.STACKACCESS.sysname.TCPIP CL(SERVAUTH) ID(ftpprofile) ACC(READ)

PE EZB.INITSTACK.** CL (SERVAUTH) ID(authusers) ACC(READ)

The following notes apply to these controls:

- EZB.STACKACCESS.sysname.TCPIP access READ should be limited to only those started tasks that require access to the TCPIP Stack as well as any users approved for FTP Access (inbound and/or outbound). FTP users should not have access to the EZB.FTP.sysname.ftpstc.ACCESS.HFS resource unless specific written justification documenting valid requirement for those FTP users to access USS files and directories via FTP.

- To be effective in restricting access, the network (EZB.NETACCESS) resource control requires configuration of the NETACCESS statement in the PROFILE.TCPIP file.

- To be effective in restricting access, the port (EZB.PORTACCESS) resource control requires configuration of a PORT or PORTRANGE statement in the PROFILE.TCPIP file. These port definitions within PROFILE.TCPIP must be defined to include SAF keyword and a valid name.

A list of possible SERVAUTH resources defined to the first two nodes is shown here: (Note that additional resources may be developed with each new release of TCPIP.)

EZA.DCAS.
EZB.BINDVIPARANGE.
EZB.CIMPROV.

EZB.FRCAACCESS.
EZB.FTP.
EZB.INITSTACK.
EZB.IOCTL.
EZB.IPSECCMD.
EZB.MODDVIPA.
EZB.NETACCESS.
EZB.NETMGMT.
EZB.NETSTAT.
EZB.NSS.
EZB.NSSCERT.
EZB.OSM.
EZB.PAGENT.
EZB.PORTACCESS.
EZB.RPCBIND.
EZB.SOCKOPT.
EZB.SNMPAGENT.
EZB.STACKACCESS.
EZB.TN3270.
IST.NETMGMT.

CCI: CCI-000213

Group ID (Vulid): V-223824

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223824r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-TC-000050](#)

Rule Title: The IBM RACF SERVAUTH resource class must be active for TCP/IP resources.

Legacy ID: V-98355

Legacy ID: SV-107459

Vulnerability Discussion: IBM Provides the SERVAUTH Class for use in protecting a variety of TCP/IP features/functions/products both IBM and third-party. Failure to activate this class will result in unprotected resources. This exposure may threaten the integrity of the operating system environment, and compromise the confidentiality of customer data.

Check Content:

From a command input screen enter:
SETROPTS LIST

If there are TCP/IP resources defined and the SERVAUTH resource class is not active, this is a

finding.

Fix Text: Configure RACF SETROPTS to have the SERVAUTH resource class is active.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below:

The RACF Command SETR LIST will show the status of RACF Controls including a list of ACTIVE classes.

The SERVAUTH Class is activated with the command SETR CLASSACT (SERVAUTH).

Generic profiles and commands should also be enabled with the command SETR GENERIC(SERVAUTH) GENCMD(SERVAUTH).

CCI: CCI-000213

Group ID (Vulid): V-223826

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223826r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-TC-000070](#)

Rule Title: IBM z/OS data sets for the Base TCP/IP component must be properly protected.

Legacy ID: V-98359

Legacy ID: SV-107463

Vulnerability Discussion: MVS data sets of the Base TCP/IP component provide the configuration, operational, and executable properties of IBM's TCP/IP system product. Failure to properly secure these data sets may lead to unauthorized access resulting in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

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

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

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

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

Check Content:

Execute a dataset access list for Base TCP/IP component datasets.

If 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-223827

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223827r868879_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-TC-000080](#)

Rule Title: IBM z/OS Configuration files for the TCP/IP stack must be properly specified.

Legacy ID: V-98361

Legacy ID: SV-107465

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

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

Check Content:

Refer to the procedure libraries defined to JES2 and locate the TCPIP JCL member.

Note:

If GLOBALTCPIPDATA is specified, any TCPIP.DATA statements contained in the specified file or data set take precedence over any TCPIP.DATA statements found using the appropriate environment's (native MVS or z/OS UNIX) search order.

If GLOBALTCPIPDATA is not specified, the appropriate environment's (Native MVS or z/OS UNIX) search order is used to locate TCPIP.DATA.

If the PROFILE and SYSTCPD DD statements specify the TCP/IP Profile and Data configuration files respectively, this not a finding.

If the RESOLVER_CONFIG variable on the EXEC statement is set to the same file name specified on the SYSTCPD DD statement, this is not a finding.

Fix Text: Review the TCP/IP started task JCL to ensure the configuration file names are specified on the appropriate DD statements and parameter option.

During initialization the TCP/IP stack uses fixed search sequences to locate the PROFILE.TCPIP and TCPIP.DATA files. However, uncertainty is reduced and security auditing is enhanced by explicitly specifying the locations of the files. In the TCP/IP started task's JCL, Data Definition (DD) statements can be used to specify the locations of the files. The PROFILE DD statement identifies the PROFILE.TCPIP file and the SYSTCPD DD statement identifies the TCPIP.DATA file.

The location of the TCPIP.DATA file can also be specified by coding the RESOLVER_CONFIG environment variable as a parameter of the ENVAR option in the TCP/IP started task's JCL. In fact, the value of this variable is checked before the SYSTCPD DD statement by some processes. However, not all processes (e.g., TN3270 Telnet Server) will access the variable to get the file location. Therefore specifying the file location explicitly, both on a DD statement and through the RESOLVER_CONFIG environment variable, reduces ambiguity.

Note:

If GLOBALTCPIPDATA is specified, any TCPIP.DATA statements contained in the specified file or data set take precedence over any TCPIP.DATA statements found using the appropriate environment's (native MVS or z/OS UNIX) search order.

If GLOBALTCPIPDATA is not specified, the appropriate environment's (Native MVS or z/OS UNIX) search order is used to locate TCPIP.DATA.

The systems programmer responsible for supporting ICS will ensure that the TCP/IP started task's JCL specifies the PROFILE and SYSTCPD DD statements for the PROFILE.TCPIP and TCPIP.DATA configuration files and TCP/IP started task's JCL includes the RESOLVER_CONFIG variable, set to the name of the file specified on the SYSTCPD DD statement.

CCI: CCI-000366

Group ID (Vulid): V-245536

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-245536r768737_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-TC-000100](#)

Rule Title: The IBM z/OS TCPIP.DATA configuration statement must contain the DOMAINORIGIN or DOMAIN specified for each TCP/IP defined.

Legacy ID: SV-107469

Legacy ID: V-98365

Vulnerability Discussion: If data origin authentication and data integrity verification are not performed, the resultant response could be forged, it may have come from a poisoned cache, the packets could have been intercepted without the resolver's knowledge, or resource records could have been removed which would result in query failure or denial of service. Data origin authentication verification must be performed to thwart these types of attacks.

Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching Domain Name System (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations.

This is not applicable if DNSSEC is not implemented on the local network.

Check Content:

Refer to the Data configuration file specified on the SYSTCPD DD statement in the TCPIP started task JCL.

Note:

If GLOBALTCPIPDATA is specified, any TCPIP.DATA statements contained in the specified file or data set take precedence over any TCPIP.DATA statements found using the appropriate environment's (native MVS or z/OS UNIX) search order.

If GLOBALTCPIPDATA is not specified, the appropriate environment's (Native MVS or z/OS UNIX) search order is used to locate TCPIP.DATA.

If the DOMAINORIGIN/DOMAIN (the DOMAIN statement is functionally equivalent to the DOMAINORIGIN statement) is specified in the TCP/IP Data configuration file, this is not a finding.

Fix Text: Configure the TCPIP.DATA file to include the DOMAINORIGIN/DOMAIN (the DOMAIN statement is functionally equivalent to the DOMAINORIGIN statement).

Note:

If GLOBALTCPIPDATA is specified, any TCPIP.DATA statements contained in the specified file or data set take precedence over any TCPIP.DATA statements found using the appropriate environment's (native MVS or z/OS UNIX) search order.

If GLOBALTCPIPDATA is not specified, the appropriate environment's (Native MVS or z/OS UNIX) search order is used to locate TCPIP.DATA.

CCI: CCI-000366

Group ID (Vulid): V-252553

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-252553r816954_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-TC-000110](#)

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 that the statements specify a FIPS 140-2 compliant value of the following values.

ECDHE_ECDSA_AES_128_CBC_SHA256
ECDHE_ECDSA_AES_256_CBC_SHA384
ECDHE_RSA_AES_128_CBC_SHA256
ECDHE_RSA_AES_256_CBC_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256

CCI: CCI-000067

Group ID (Vulid): V-223831

Group Title: SRG-OS-000033-GPOS-00014

Rule ID: SV-223831r877398_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-TN-000020](#)

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: SV-107473

Legacy ID: V-98369

Vulnerability Discussion: During the SSL connection process a mutually acceptable encryption algorithm is selected by the server and client. This algorithm is used to encrypt the data that subsequently flows between the two. However, the level or strength of encryption can vary greatly. Certain configuration options can allow no encryption to be used and others can allow a relatively weak 40-bit algorithm to be used. Failure to properly enforce adequate encryption strength could result in the loss of data privacy.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000120-GPOS-00061, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000396-GPOS-00176, SRG-OS-000478-GPOS-00223, SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190, SRG-OS-000478-GPOS-00223

Check Content:

Refer to the Profile configuration file specified on the PROFILE DD statement in the TCPIP started task JCL.

If the following items are in effect for the configuration specified in the TCP/IP Profile configuration file, this is not a finding.

NOTE: If an INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

NOTE: FIPS 140-2 minimum encryption is the accepted level of encryption and will override this requirement if greater.

The TELNETGLOBALS block that specifies an ENCRYPTION statement states one or more of the below cipher specifications.

Each TELNETPARMS block that specifies the SECUREPORT statement, specifies an ENCRYPTION statement states one or more of the below cipher specifications. And the TELNETGLOBALS block does or does not specify an ENCRYPTION statement.

Cipher Specifications

SSL_3DES_SHA

SSL_AES_256_SHA

SSL_AES_128_SHA

Fix Text: Configure the SECUREPORT and TELNETPARMS ENCRYPTION statements and/or the TELNETGLOBALS statement in the PROFILE.TCPIP file to conform to the

requirements specified below.

The TELNETGLOBALS block may specify an ENCRYPTION statement that specifies one or more of the below cipher specifications.

Each TELNETPARMS block that specifies the SECUREPORT statement, an ENCRYPTION statement is coded with one or more of the below cipher specifications. And the TELNETGLOBALS block does or does not specify an ENCRYPTION statement.

To prevent the use of non FIPS 140-2 encryption, the TELNETGLOBALS block and/or each TELNETPARMS block that specifies an ENCRYPTION statement will specify one or more of the following cipher specifications:

Cipher Specifications

SSL_3DES_SHA

SSL_AES_256_SHA

SSL_AES_128_SHA

Note: Always check for the minimum allowed in FIPS 140-2.

CCI: CCI-000068

CCI: CCI-000803

CCI: CCI-001453

CCI: CCI-002418

CCI: CCI-002420

CCI: CCI-002421

CCI: CCI-002422

CCI: CCI-002450

CCI: CCI-002890

CCI: CCI-003123

Group ID (Vulid): V-223833

Group Title: SRG-OS-000228-GPOS-00088

Rule ID: SV-223833r803642_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-TN-000040](#)

Rule Title: The IBM z/OS warning banner for the TN3270 Telnet server must contain the proper content of the Standard Mandatory DoD Notice and Consent Banner.

Legacy ID: SV-107477

Legacy ID: V-98373

Vulnerability Discussion: 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:

Refer to the Profile configuration file specified on the PROFILE DD statement in the TN3270 started task JCL.

If all USS tables referenced in BEGINVTAM USSTCP statements include MSG10 text that specifies the Standard logon banner, this is not a finding.

The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

DOD requires that a logon warning banner be displayed. Within the TN3270 Telnet Server, the banner can be implemented through the USS table that is specified on a BEGINVTAM USSTCP statement. The text associated with message ID 10 (i.e., MSG10) in the USS table is sent to clients that are subject to USSTCP processing.

Fix Text: Review all USS tables referenced in BEGINVTAM USSTCP statements in the PROFILE.TCPIP file. Ensure the MSG10 text specifies a logon banner in accordance with DISA requirements. See required MSG10 content below:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI

investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

DOD requires that a logon warning banner be displayed. Within the TN3270 Telnet Server, the banner can be implemented through the USS table that is specified on a BEGINVTAM USSTCP statement. The text associated with message ID 10 (i.e., MSG10) in the USS table is sent to clients that are subject to USSTCP processing.

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

CCI: CCI-000048

CCI: CCI-000050

Group ID (Vulid): V-223834

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223834r868882_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-TN-000050](#)

Rule Title: IBM z/OS VTAM session setup controls for the TN3270 Telnet server must be properly specified.

Legacy ID: V-98375

Legacy ID: SV-107479

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal

standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

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

Check Content:

Refer to the TN3270 Profile configuration file identified by the PROFILE DD in the TN3270 procedure.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

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

If any of the 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-223835

Group Title: SRG-OS-000163-GPOS-00072

Rule ID: SV-223835r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-TN-000060](#)

Rule Title: The IBM z/OS PROFILE.TCPIP configuration for the TN3270 Telnet server must have the INACTIVE statement properly specified.

Legacy ID: V-98377

Legacy ID: SV-107481

Vulnerability Discussion: Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Check Content:

Refer to the Profile configuration file specified on the PROFILE DD statement in the TN3270 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.

TELNETGLOBAL Block (only one defined)

TELNETPARMS Block (one defined for each port the server is listening to, typically ports 23 and 992)

If the TELNETPARMS INACTIVE statement is coded either in the TELNETGLOBALS or within each TELNETPARMS statement block and specifies a value between "1" and "900", this is not a finding.

Fix Text: Configure the configuration statements in the PROFILE.Tn3270 to conform to the specifications below:

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

The TELNETPARMS INACTIVE statement is coded either within the TELNETGLOBALS OR within each TELNETPARMS statement block and specifies a value between "1" and "900".

CCI: CCI-001133

Group ID (Vulid): V-223836

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223836r868884_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-TS-000010](#)

Rule Title: IBM Z/OS TSOAUTH resources must be restricted to authorized users.

Legacy ID: V-98379

Legacy ID: SV-107483

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:

RLIST SURROGAT *

Ensure that all TSOAUTH resources and/or generic equivalent are properly protected according to the requirements specified.

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

The ACCT authorization is restricted to security personnel.

The CONSOLE authorization is restricted to authorized systems personnel (e.g., systems programming personnel, operations staff, etc.) and READ access may be given to all user when SDSF is installed at the ISSOs discretion.

The MOUNT authorization is restricted to DASD batch users only.

The OPER authorization is restricted to authorized systems personnel (e.g., systems programming personnel, operations staff, etc.).

The PARMLIB authorization is restricted to only z/OS systems programming personnel and READ access may be given to auditors.

The TESTAUTH authorization is restricted to only z/OS systems programming personnel.

Fix Text: Configure the TSOAUTH resource class to control sensitive TSO/E commands.

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

Below is listed the access requirements for TSOAUTH resources. Ensure the guidelines for the resources and/or generic equivalent are followed.

The ACCT authorization is restricted to security personnel.

The CONSOLE authorization is restricted to authorized systems personnel (e.g., systems programming personnel, operations staff, etc.) and READ access may be given to all user when SDSF is installed 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-223837

Group Title: SRG-OS-000324-GPOS-00125

Rule ID: SV-223837r877392_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-TS-000020](#)

Rule Title: IBM RACF LOGONIDs must not be defined to SYS1.UADS for non-emergency use.

Legacy ID: V-98381

Legacy ID: SV-107485

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:

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-223838

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223838r604139_rule

Severity: CAT I

Rule Version (STIG-ID): [RACF-US-000010](#)

Rule Title: The IBM z/OS UNIX SUPERUSER resources must be protected in accordance with guidelines.

Legacy ID: V-98383

Legacy ID: SV-107487

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:

```
RL UNIXPRIV * AUTHUSER
```

If the RACF rules for the SUPERUSER resource specify a default access of NONE, this is not a finding.

If there are no RACF rules that allow access to the SUPERUSER resource, this is not a finding.

If there is no RACF rule for CHOWN.UNRESTRICTED defined, this is not a finding.

If the RACF 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 RACF rules for each of the SUPERUSER resources listed in the z/OS UNIX System Services Planning, Establishing UNIX security, restrict access to appropriate system tasks or systems programming personnel, this is not a finding.

Fix Text: Configure all SUPERUSER resources for the UNIXPRIV resource class to be restricted to appropriate system tasks and/or system programming personnel.

- The RACF rules for the SUPERUSER resource specify a default access of NONE.
- There are no RACF rules that allow access to the SUPERUSER resource.
- There is no RACF rule for CHOWN.UNRESTRICTED defined.
- The RACF 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.
- The RACF rules for each of the SUPERUSER resources listed in the z/OS UNIX System Services Planning, Establishing UNIX security, restrict access to appropriate system tasks or systems programming personnel.

Sample Commands:

```
RDEF UNIXPRIV SUPERUSER.** UACC(NONE) OWNER(ADMIN) DATA('REFERENCE  
ZUSS0023') AUDIT(ALL(READ))
```

```
/* do not permit any users/groups to this resource */
```

```
SR CLASS(UNIXPRIV) MASK(CHOWN.UNRESTRICTED)
```

```
/* delete if found */
```

```
PE SUPERUSER.FILESYS.** CL(UNIXPRIV) ID(<SYSPsmpl>)
```

CCI: CCI-000213

Group ID (Vulid): V-223839

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223839r767099_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000020](#)

Rule Title: IBM z/OS BPX resource(s) must be protected in accordance with security requirements.

Legacy ID: V-98385

Legacy ID: SV-107489

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:

```
RL FACILITY * AUTHUSER
```

If the RACF rules for the BPX.** resource specify a default access of NONE, this is not a finding.

If there are no RACF user access to the BPX.** resource, this is not a finding.

If there is no RACF rule for BPX.SAFFASTPATH defined, this is not a finding.

If the RACF rules for each of the BPX resources listed in the z/OS UNIX System Services Planning, Establishing UNIX security, restrict access to appropriate system tasks or systems programming personnel, this is not a finding.

Fix Text: There are a number of resources available under z/OS UNIX that must be secured in order to preserve system integrity while allowing effective application and user access. All of these resources might not be used in every configuration, but several of them have critical impacts.

The default access for each of these resources must be no access. A generic resource (e.g., BPX.***) must also be set to a default access of none to cover future additions. Because they convey especially powerful privileges, the settings for BPX.DAEMON, BPX.SAFFASTPATH, BPX.SERVER, and BPX.SUPERUSER require special attention.

Access to BPX.DAEMON must be restricted to the z/OS UNIX kernel userid, z/OS UNIX daemons (e.g., inetd, syslogd, ftpd), and other system software daemons (e.g., web servers).

As noted above, the BPX.SAFFASTPATH definition can cause successful security checks not to be audited. Because auditing of all accesses is required for some system files, BPX.SAFFASTPATH must not be used.

Access to BPX.SERVER must be restricted to system software processes that act as servers under z/OS UNIX (e.g., web servers).

Access to BPX.SUPERUSER must be restricted to Security Administrators and individual systems programming personnel. It is not appropriate for all systems programming personnel, only for those with responsibilities for components or products that use z/OS UNIX and that

require superuser capability for maintenance.

- The RACF rules for the BPX.** resource specify a default access of NONE.
- There are no RACF user access to the BPX.** resource.
- There is no RACF rule for BPX.SAFFASTPATH defined.
- The RACF rules for each of the BPX resources specify a UACC value of NONE.
- The RACF rules for each of the BPX resources restrict access to appropriate system tasks or systems programming personnel as specified.

The following list of sample commands is provided to implement this requirement:

```
rdef facility bpx.** UACC(none) owner(admin) audit(all(read)) - data('see zuss0021')
rdef facility bpx.daemon UACC(none) owner(admin) -
audit(all(read)) data('see zuss0021')
pe bpx.daemon cl(facility id(<authorized_users>))
rdef facility bpx.debug UACC(none) owner(admin) -
audit(all(read)) data('see zuss0021')
pe bpx.debug cl(facility id(<authorized_users>))
rdef facility bpx.fileattr.apf UACC(none) owner(admin) -
audit(all(read)) data('see zuss0021')
pe bpx.fileattr.apf cl(facility id(<authorized_users>))
rdef facility bpx.fileattr.progctl UACC(none) owner(admin) -
audit(all(read)) data('see zuss0021')
pe bpx.fileattr.progctl cl(facility id(<authorized_users>))
rdef facility bpx.jobname UACC(none) owner(admin) -
audit(all(read)) data('see zuss0021')
pe bpx.jobname cl(facility id(<authorized_users>))
rdef facility bpx.server UACC(none) owner(admin) -
audit(all(read)) data('see zuss0021')
pe bpx.server cl(facility id(<authorized_users>))
rdef facility bpx.smf UACC(none) owner(admin) -
audit(all(read)) data('see zuss0021')
pe bpx.smf cl(facility id(<authorized_users>))
rdef facility bpx.stor.swap UACC(none) owner(admin) -
audit(all(read)) data('see zuss0021')
pe bpx.stor.swap cl(facility id(<authorized_users>))
rdef facility bpx.superuser UACC(none) owner(admin) -
audit(all(read)) data('see zuss0021')
pe bpx.superuser cl(facility id(<authorized_users>))
rdef facility bpx.wlmsserver UACC(none) owner(admin) -
audit(all(read)) data('see zuss0021')
pe bpx.wlmsserver cl(facility id(<authorized_users>))
```

CCI: CCI-000213

Group ID (Vulid): V-223840

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223840r868887_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000030](#)

Rule Title: IBM z/OS UNIX MVS HFS directories with other write permission bit set must be properly defined.

Legacy ID: SV-107491

Legacy ID: V-98387

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:

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-223842

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223842r868890_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000050](#)

Rule Title: IBM z/OS UNIX security parameters in etc/profile must be properly specified.

Legacy ID: SV-107495

Legacy ID: V-98391

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

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements.

Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Check Content:

From the ISPF Command Shell enter:

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, the LOGNAME variable is marked read-only for the /etc/profile file, and exceptions are documented with the ISSO.

CCI: CCI-000213

Group ID (Vulid): V-223843

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223843r868893_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000060](#)

Rule Title: IBM z/OS UNIX security parameters in /etc/rc must be properly specified.

Legacy ID: V-98393

Legacy ID: SV-107497

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

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

Check Content:

From the ISPF Command Shell enter:

ISHELL

/etc/rc

If all of the CHMOD commands in /etc/rc do not result in less restrictive access than what is specified in the tables below, this is not a finding.

NOTE: The use of CHMOD commands in /etc/rc is required in most environments to comply with the required settings, especially for dynamic objects such as the /dev directory.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)

6 rw-

3 -wx

2 -w-

5 r-x

4 r--

1 --x

0 --- (most restrictive)

If all of the CHAUDIT commands in /etc/rc do not result in less auditing than what is specified in the tables below, this is not a finding.

NOTE: The use of CHAUDIT commands in /etc/rc may not be necessary. If none are found, there is not a finding.

The possible audit bits settings are as follows:

f log for failed access attempts

a log for failed and successful access

- no auditing

If the _BPX_JOBNAME variable is appropriately set (i.e., to match daemon name) as each daemon (e.g., syslogd, inetd) is started in /etc/rc, this is not a finding.

NOTE: If _BPX_JOBNAME is not specified, the started address space will be named using an inherited value. This could result in reduced security in terms of operator command access.

SYSTEM DIRECTORY SECURITY SETTINGS**DIRECTORY PERMISSION BITS USER AUDIT BITS FUNCTION**

/ [root] 755 faf Root level of all file systems. Holds critical mount points.

/bin 1755 fff Shell scripts and executables for basic functions

/dev 1755 fff Character-special files used when logging into the OMVS shell and during C language program compilation.
Files are created during system IPL and on a per-demand basis.
/etc 1755 faf Configuration programs and files (usually with locally customized data) used by z/OS UNIX and other product initialization processes
/lib 1755 fff System libraries including dynamic link libraries and files for static linking
/samples 1755 fff Sample configuration and other files
/tmp 1777 fff Temporary data used by daemons, servers, and users. Note: /tmp must have the sticky bit on to restrict file renames and deletions.
/u 1755 fff Mount point for user home directories and optionally for third-party software and other local site files
/usr 1755 fff Shell scripts, executables, help (man) files and other data. Contains sub-directories (e.g., lpp) and mount points used by program products that may be in separate file systems.
/var 1775 fff Dynamic data used internally by products and by elements and features of z/OS UNIX.

SYSTEM FILE SECURITY SETTINGS

FILE PERMISSION BITS USER AUDIT BITS FUNCTION

/bin/sh 1755 faf z/OS UNIX shell
Note: /bin/sh has the sticky bit on to improve performance.
/dev/console 740 fff The system console file receives messages that may require System Administrator (SA) attention.
/dev/null 666 fff A null file; data written to it is discarded.
/etc/auto.master and
any mapname files 740 faf Configuration files for automount facility
/etc/inetd.conf 740 faf Configuration file for network services
/etc/init.options 740 faf Kernel initialization options file for z/OS UNIX environment
/etc/log 744 fff Kernel initialization output file
/etc/profile 755 faf Environment setup script executed for each user
/etc/rc 744 faf Kernel initialization script for z/OS UNIX environment
/etc/steplib 740 faf List of MVS data sets valid for set user ID and set group ID executables
/etc/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

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-223844

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223844r853638_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000070](#)

Rule Title: IBM z/OS UNIX resources must be protected in accordance with security requirements.

Legacy ID: SV-107499

Legacy ID: V-98395

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

Access control policies include: identity-based policies, role-based policies, and attribute-based

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

Satisfies: SRG-OS-000080-GPOS-00048, SRG-OS-000326-GPOS-00126

Check Content:

From the ISPF Command Shell enter:

```
RL SURROGAT BPX.SRV AUTHUSER
```

If the RACF rules for all BPX.SRV.user SURROGAT resources specify a default access of NONE, this is not a finding.

If the RACF rules for all BPX.SRV.user SURROGAT resources restrict access to system software processes (e.g., web servers) that act as servers under z/OS UNIX, this is not a finding.

If the RACF rules for all BPX.SRV.user SURROGAT resources restrict access to authorized users identified in the Site Security Plan, this is not a finding.

Fix Text: 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.

Configure 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 z/OS UNIX (e.g., web servers) and users whose access and approval are identified in the Site Security Plan.

A sample is provided here:

```
RDEF SURROGAT BPX.SRV.user UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
```

-RACF rules for all BPX.SRV.user SURROGAT resources must restrict access to system software processes (e.g., web servers) that act as servers under z/OS UNIX.

```
RDEF SURROGAT BPX.SRV.user UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))  
PE BPX.SRV.user CL(SURROGAT) ID(<server>)
```

CCI: CCI-000213

CCI: CCI-002233

Group ID (Vulid): V-223845

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223845r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000080](#)

Rule Title: IBM z/OS UNIX MVS data sets or HFS objects must be properly protected.

Legacy ID: V-98397

Legacy ID: SV-107501

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

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

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

Check Content:

Refer to the proper BPXPRMxx member in SYS1.PARMLIB

If the ESM data set rules for the data sets referenced in the ROOT and the MOUNT statements in BPXPRMxx restrict update access to the z/OS UNIX kernel (i.e., OMVS or OMVSKERN), this is not a finding.

If the ESM data set rules for the data set referenced in the ROOT and the MOUNT statements in BPXPRMxx restrict 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 set 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-223846

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223846r868895_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000090](#)

Rule Title: IBM z/OS UNIX MVS data sets WITH z/OS UNIX COMPONENTS must be properly protected.

Legacy ID: V-98399

Legacy ID: SV-107503

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:

Execute an access list for MVS DATA SETS WITH z/OS UNIX COMPONENTS.

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-223847

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223847r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000100](#)

Rule Title: IBM z/OS UNIX HFS permission bits and audit bits for each directory must be properly protected.

Legacy ID: V-98401

Legacy ID: SV-107505

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

enter CD /

enter ls -alW

If the HFS permission bits and user audit bits for each directory and file match or are more restrictive than the specified settings listed in the SYSTEM DIRECTORY SECURITY SETTINGS table below, this is not a finding.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)

6 rw-

3 -wx

2 -w-

5 r-x

4 r--

1 --x

0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts

a log for failed and successful access

- no auditing

SYSTEM DIRECTORY SECURITY SETTINGS

DIRECTORY PERMISSION BITS USER AUDIT BITS FUNCTION

/ [root] 755 faf Root level of all file systems. Holds critical mount points.
 /bin 1755 fff Shell scripts and executables for basic functions
 /dev 1755 fff Character-special files used when logging into the OMVS shell and during C language program compilation.
 Files are created during system IPL and on a per-demand basis.
 /etc 1755 faf Configuration programs and files (usually with locally customized data) used by z/OS UNIX and other product initialization processes
 /lib 1755 fff System libraries including dynamic link libraries and files for static linking
 /samples 1755 fff Sample configuration and other files
 /tmp 1777 fff Temporary data used by daemons, servers, and users. Note: /tmp must have the sticky bit on to restrict file renames and deletions.
 /u 1755 fff Mount point for user home directories and optionally for third-party software and other local site files
 /usr 1755 fff Shell scripts, executables, help (man) files and other data. Contains sub-directories (e.g., lpp) and mount points used by program products that may be in separate file systems.
 /var 1775 fff Dynamic data used internally by products and by elements and features of z/OS UNIX.

Fix Text: Configure the UNIX permission bits and user audit bits on each of the HFS directories in the table SYSTEM DIRECTORY SECURITY SETTINGS below to be equal or more restrictive.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx (least restrictive)
 6 rw-
 3 -wx
 2 -w-
 5 r-x
 4 r--
 1 --x
 0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
 a log for failed and successful access
 - no auditing

SYSTEM DIRECTORY SECURITY SETTINGS

DIRECTORY PERMISSION BITS USER AUDIT BITS FUNCTION

/ [root] 755 faf Root level of all file systems. Holds critical mount points.
 /bin 1755 fff Shell scripts and executables for basic functions
 /dev 1755 fff Character-special files used when logging into the OMVS shell and during C language program compilation.
 Files are created during system IPL and on a per-demand basis.

/etc 1755 faf Configuration programs and files (usually with locally customized data) used by z/OS UNIX and other product initialization processes
/lib 1755 fff System libraries including dynamic link libraries and files for static linking
/samples 1755 fff Sample configuration and other files
/tmp 1777 fff Temporary data used by daemons, servers, and users. Note: /tmp must have the sticky bit on to restrict file renames and deletions.
/u 1755 fff Mount point for user home directories and optionally for third-party software and other local site files
/usr 1755 fff Shell scripts, executables, help (man) files and other data. Contains sub-directories (e.g., lpp) and mount points used by program products that may be in separate file systems.
/var 1775 fff Dynamic data used internally by products and by elements and features of z/OS UNIX.

The following commands are a sample of the commands to be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

```
chmod 0755 /  
chaudit w=sf,rx+f /  
chmod 0755 /bin  
chaudit rwx=f /bin
```

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-223848

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223848r868898_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000110](#)

Rule Title: IBM z/OS UNIX SYSTEM FILE SECURITY SETTINGS must be properly protected or specified.

Legacy ID: V-98403

Legacy ID: SV-107507

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.

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

Check Content:

From the ISPF Command Shell enter:
OMVS

For each file listed in the table below enter:
ls -alW /<directory name>/<file name>

If the HFS permission bits and user audit bits for each directory and file match or are more restrictive than the specified settings listed in the table, this is not a finding.

NOTE: Some of the files listed are not used in every configuration. Absence of any of the files is not considered a finding.

SYSTEM FILE SECURITY SETTINGS**FILE PERMISSION BITS USER AUDIT BITS FUNCTION**

/bin/sh 1755 faf z/OS UNIX shell

Note: /bin/sh has the sticky bit on to improve performance.

/dev/console 740 fff The system console file receives messages that may require System Administrator (SA) attention.

/dev/null 666 fff A null file; data written to it is discarded.

/etc/auto.master

any mapname files 740 faf Configuration files for automount facility

/etc/inetd.conf 740 faf Configuration file for network services

/etc/init.options 740 faf Kernel initialization options file for z/OS UNIX environment

/etc/log 744 fff Kernel initialization output file

/etc/profile 755 faf Environment setup script executed for each user

/etc/rc 744 faf Kernel initialization script for z/OS UNIX environment

/etc/steplib 740 faf List of MVS data sets valid for set user ID and set group ID executables

/etc/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-223849

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223849r853639_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000120](#)

Rule Title: IBM z/OS UNIX MVS data sets used as step libraries in /etc/steplib must be properly protected.

Legacy ID: V-98405

Legacy ID: SV-107509

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

authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

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

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

Check Content:

Refer to the pathname from the STEPLIBLIST line in BPXPRMxx member of PARMLIB.

From the ISPF Command Shell enter:

ISHELL

On the command line:

on the path name line enter:

/etc/

From the resulting display scroll down to the <stepliblist name> from BPXPRMxx parm. Enter B for browse on that line.

If ESM data set rules for libraries specified restrict WRITE or greater access to only systems programming personnel, this is not a finding.

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

Fix Text: Configure WRITE or greater access to libraries residing in the /etc/steplib to be limited to system programmers only.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002235

Group ID (Vulid): V-223850

Group Title: SRG-OS-000326-GPOS-00126

Rule ID: SV-223850r853640_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000130](#)

Rule Title: The IBM RACF classes required to properly secure the z/OS UNIX environment must be ACTIVE.

Legacy ID: SV-107511

Legacy ID: V-98407

Vulnerability Discussion: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned by the organizations.

Check Content:

From the ISPF Command Shell enter:

SETRopts list

If the ACTIVE CLASSES list includes entries for the FACILITY, SURROGAT, and UNIXPRIV resource classes, this is not a finding.

If either of the above resource classes is missing, this is a finding.

Fix Text: Define the ACTIVE CLASS Parameter in SETROPTS to include the FACILITY, SURROGAT and UNIXPRIV resource classes.

EXAMPLES:

SETR CLASSACT(FACILITY SURROGAT UNIXPRIV)

SETR GENERIC(FACILITY SURROGAT UNIXPRIV)

SETR GENCMD(FACILITY SURROGAT UNIXPRIV)

SETR RACL(FACILITY SURROGAT UNIXPRIV)

CCI: CCI-002233

Group ID (Vulid): V-223851

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223851r868901_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000140](#)

Rule Title: IBM z/OS UNIX OMVS parameters in PARMLIB must be properly specified.

Legacy ID: SV-107513

Legacy ID: V-98409

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

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

Check Content:

Refer to the IEASYS00 member of SYS1.PARMLIB.

If the parameter is specified as OMVS=xx or OMVS=(xx,xx,...) in the IEASYSxx member, this is not a finding.

If the OMVS statement is not specified, OMVS=DEFAULT is used. In minimum mode there is no access to permanent file systems or to the shell, and IBM's Communication Server TCP/IP will not run.

Fix Text: Configure the settings in PARMLIB and /etc for z/OS UNIX security parameters with values that conform to the specifications below:

The parameter is specified as OMVS=xx or OMVS=(xx,xx,...) in the IEASYSxx member.

Note: If the OMVS statement is not specified, OMVS=DEFAULT is used. In minimum mode there is no access to permanent file systems or to the shell, and IBM's Communication Server TCP/IP will not run.

CCI: CCI-000366

Group ID (Vulid): V-223852

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223852r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000150](#)

Rule Title: IBM z/OS UNIX BPXPRMxx security parameters in PARMLIB must be properly specified.

Legacy ID: SV-107515

Legacy ID: V-98411

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 BPXPRM00 member of SYS1.PARMLIB.

If the required parameter keywords and values are defined as detailed below, this is not a finding.

Parameter Keyword Value
SUPERUSER BPXROOT
TTYGROUP TTY
STEPLIBLIST /etc/steplib
USERIDALIASTABLE Will not be specified.
ROOT SETUID will be specified
MOUNT NOSETUID
SETUID (for Vendor-provided files)SECURITY
STARTUP_PROC OMVS

Fix Text: Define the settings in PARMLIB member BPXPRMxx for z/OS UNIX security parameters values to conform to the specifications below:

Parameter Keyword Value
SUPERUSER BPXROOT
TTYGROUP TTY
STEPLIBLIST /etc/steplib
USERIDALIASTABLE Will not be specified.
ROOT SETUID will be specified
MOUNT NOSETUIDSETUID (for Vendor-provided files)SECURITY
STARTUP_PROC OMVS

CCI: CCI-000366

Group ID (Vulid): V-223853

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223853r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000160](#)

Rule Title: IBM z/OS default profiles must be defined in the corresponding FACILITY Class Profile for classified systems.

Legacy ID: V-98413

Legacy ID: SV-107517

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:

If the system is not classified, this is Not Applicable.

From a command input screen enter:

```
RLIST FACILITY (BPX.UNIQUE.USER) ALL  
Examine APPLICATION DATA for userid
```

If system is classified and a userid is are not defined in the Application Data field in the BPX.UNIQUE.USER resource in the FACILITY report, this is not a finding.

Fix Text: If system is classified a userid should not be defined in the application data field of the FACILITY report.

The sample commands below show the required security parameters required for the default user:

AU OEDFLTU DFLTGRP(OEDFLTG) NAME('OE DEFAULT USER') NOPASS -
OMVS(UID(99999) HOME('/u/oeflt') PROGRAM('/bin/echo')) -
DATA('DEFAULT OMVSUSERID ADDED WITH SOER5')

RDEF FACILITY BPX. UNIQUE.USER APPLDATA() -
DATA('ADDED TO SUPPORT THE DEFAULT USER') UACC(NONE) OWNER(ADMIN)

SETR RACLIST(FACILITY) REFRESH

CCI: CCI-000366

Group ID (Vulid): V-223854

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-223854r868904_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000170](#)

Rule Title: IBM z/OS UNIX HFS MapName files security parameters must be properly specified.

Legacy ID: V-98415

Legacy ID: SV-107519

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-223855

Group Title: SRG-OS-000096-GPOS-00050

Rule ID: SV-223855r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-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-98417

Legacy ID: SV-107521

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 specified but not commented out, this is a finding.

RESTRICTED NETWORK SERVICES/PORTS

Service Port

Chargen 19

Daytime 13

Discard 9

Echo 7

Exec 512

finger 79

shell 514

time 37

login 513

smtp 25

timed 525

nameserver 42

systat 11

uucp 540

netstat 15

talk 517

qotd 17

tftp 69

Fix Text: Review the settings in the /etc/inetd.conf file determine if every entry in the file represents a service that is actually in use. Services that are not in use must be disabled to reduce potential security exposures.

The following services must be disabled in /etc/inetd.conf unless justified and documented with the ISSO:

RESTRICTED NETWORK SERVICES

Service Port
Chargen 19
Daytime 13
Discard 9
Echo 7
Exec 512
finger 79
shell 514
time 37
login 513
smtp 25
timed 525
nameserver 42
systat 11
uucp 540
netstat 15
talk 517
qotd 17
tftp 69

The /etc/inetd.conf file is used by the INETD daemon. It specifies how INETD is to handle service requests on network sockets. Specifically, there is one entry in inetd.conf for each service. Each service entry specifies several parameters. The login_name parameter is of special interest. It specifies the userid under which the forked daemon is to execute. This userid is defined to the ACP and it may require a UID(0) (i.e., superuser authority) value.

CCI: CCI-000382

Group ID (Vulid): V-223856
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-223856r604139_rule
Severity: CAT I
Rule Version (STIG-ID): [RACF-US-000190](#)

Rule Title: IBM z/OS UID(0) must be properly assigned.

Legacy ID: V-98419

Legacy ID: SV-107523

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 a z/OS command screen enter:

```
SR CLASS(USER) UID(0)
```

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 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: Assign UID(0) 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-223857

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-223857r868907_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000200](#)

Rule Title: IBM z/OS UNIX groups must be defined with a unique GID.

Legacy ID: V-98421

Legacy ID: SV-107525

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. RACF userid groups, and started tasks that use z/OS UNIX facilities are defined to an ACP with attributes including UID and GID. If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Check Content:

From ISPF Command Shell enter:

Listgrp * OMVS

If each group is defined with a unique GID, this is not a finding.

Note: A site can choose to have both an OMVSGRP group and an STCOMVS group or combine the groups under one of these names.

If OMVSGRP and/or STCOMVS groups are defined and have a unique GID in the range of 1-99, this is not a finding.

Fix Text: Define each UNIX group with a unique GID.

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-223859

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-223859r868910_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000220](#)

Rule Title: The IBM z/OS user account for the UNIX kernel (OMVS) must be properly defined to the security database.

Legacy ID: V-98425

Legacy ID: SV-107529

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.

Check Content:

If OMVS userid is defined to the ESM as follows, this is not a finding.

No access to interactive on-line facilities (e.g., TSO, CICS, etc.)

Default group specified as OMVSGRP or STCOMVS

UID(0)

HOME directory specified as "/"

Shell program specified as "/bin/sh"

Fix Text: Define OMVS userid to the ESM as specified below:

No access to interactive on-line facilities (e.g., TSO, CICS, etc.)

Default group specified as OMVSGRP or STCOMVS

UID(0)

HOME directory specified as "/"

Shell program specified as "/bin/sh"

CCI: CCI-000764

Group ID (Vulid): V-223860

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-223860r868913_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000230](#)

Rule Title: The IBM z/OS user account for the z/OS UNIX SUPERUSER userid must be properly defined.

Legacy ID: SV-107531

Legacy ID: V-98427

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

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

- 1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and
- 2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Check Content:

Refer to system PARMLIB member BPXPRMxx (xx is determined by OMVS entry in IEASYS00.)

Determine the user ID identified by the SUPERUSER parameter. (BPXROOT is the default).

From a command input screen enter:

LISTUSER (superuser userid) TSO CICS OMVS

If the SUPERUSER userid is defined as follows, this is not a finding:

- No access to interactive on-line facilities (e.g., TSO, CICS, etc.)
- Default group specified as OMVSGRP or STCOMVS
- UID(0)
- HOME directory specified as "/"
- Shell program specified as "/bin/sh"

Fix Text: Define the user ID identified in the BPXPRM00 SUPERUSER parameter as specified below:

- No access to interactive on-line facilities (e.g., TSO, CICS, etc.)
- Default group specified as OMVSGRP or STCOMVS
- UID(0)
- HOME directory specified as "/"
- Shell program specified as "/bin/sh"

CCI: CCI-000764

Group ID (Vulid): V-223861

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-223861r868916_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000240](#)

Rule Title: The IBM z/OS user account for the UNIX (RMFGAT) must be properly defined.

Legacy ID: SV-107533

Legacy ID: V-98429

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 defined, this is Not Applicable.

From a command input screen enter:

LISTUSER (RMFGAT) 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-223862

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-223862r868919_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000250](#)

Rule Title: IBM z/OS UNIX user accounts must be properly defined.

Legacy ID: SV-107535

Legacy ID: V-98431

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 a z/OS command screen enter:

```
LISTUSER * OMVS NORACF
```

NOTE: This check only applies to users of z/OS UNIX (i.e., users with an OMVS profile defined).

If each user account with an OMVS segment is defined as follows, this is not a finding.

- A unique UID number (except for UID(0) users)
- A unique HOME directory (except for UID(0) and other system task accounts)
- Shell program specified as "/bin/sh", "/bin/tcsh", "/bin/echo", or "/bin/false"

NOTE: The shell program must have one of the specified values. The HOME directory must have a value (i.e., not be allowed to default).

Fix Text: Define users of z/OS UNIX (i.e., users with an OMVS profile defined) 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-223863

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-223863r868922_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-US-000260](#)

Rule Title: IBM z/OS attributes of UNIX user accounts used for account modeling must be defined in accordance with security requirements.

Legacy ID: V-98433

Legacy ID: SV-107537

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, and there is an account used for modeling, this is a finding.

From a command input screen enter:

```
RLIST FACILITY (BPX.UNIQUE.USER) ALL
```

Examine APPLICATION DATA for userid

Enter:

```
List User (<userid>)
```

Note: This check applies to any user id used to model OMVS access on the mainframe. This includes the OMVS default user and BPX.UNIQUE.USER. If the OMVS default user or BPX.UNIQUE.USER is not defined in the FACILITY report, this is Not Applicable.

If user account used for OMVS account modeling 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: Use of the OMVS default UID will not be allowed on any Classified system. This is not an issue when using BPX.UNIQUE.USER.

Define user id used for OMVS account modeling with a non-0 UID, a nonwritable home directory, such as "\" root, and a nonexecutable, but existing, binary file, "/bin/false" or "/bin/echo."

CCI: CCI-000764

Group ID (Vulid): V-223864

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223864r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-UT-000010](#)

Rule Title: The IBM z/OS startup user account for the z/OS UNIX Telnet Server must be properly defined.

Legacy ID: V-98435

Legacy ID: SV-107539

Vulnerability Discussion: The PROFILE.TCPIP configuration file provides system operation and configuration parameters for the TN3270 Telnet Server. Several of these parameters have potential impact to system security. Failure to code the appropriate values could result in unexpected operations and degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Check Content:

From the ISPF Command Shell enter:

```
omvs
```

```
cd /etc
```

```
cat inetd.conf
```

If the otelnetd command specifies any user other than OMVS or OMVSKERN, this is a finding.

Fix Text: The user account used at the startup of otelnetd is specified in the inetd configuration file. This account is used to perform the identification and authentication of the user requesting the session. Because the account is only used until user authentication is completed, there is no need for a unique account for this function. The z/OS UNIX kernel account can be used.

CCI: CCI-000213

Group ID (Vulid): V-223865

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223865r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-UT-000020](#)

Rule Title: IBM z/OS HFS objects for the z/OS UNIX Telnet Server must be properly protected.

Legacy ID: V-98437

Legacy ID: SV-107541

Vulnerability Discussion: HFS directories and files of the z/OS UNIX Telnet Server provide the configuration and executable properties of this product. Failure to properly secure these objects may lead to unauthorized access resulting in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

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/otelnstd 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/otelneta 1740 fff

/etc/banner 0744 faf

NOTE:

The /usr/sbin/otelneta object is a symbolic link to /usr/lpp/tcpip/sbin/otelneta. 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/otelneta
```

```
chaudit rwx=f /usr/lpp/tcpip/sbin/otelneta
```

```
chmod 0744 /etc/banner
```

```
chaudit w=sf,rx=f /etc/banner
```

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-223866

Group Title: SRG-OS-000024-GPOS-00007

Rule ID: SV-223866r695468_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-UT-000030](#)

Rule Title: The IBM z/OS UNIX Telnet Server etc/banner file must have the Standard Mandatory DoD Notice and Consent Banner.

Legacy ID: V-98439

Legacy ID: SV-107543

Vulnerability Discussion: A logon banner can be used to inform users about the environment during the initial logon. 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.

This banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Fix Text: Configure the /etc/otelnets/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-223867

Group Title: SRG-OS-000228-GPOS-00088

Rule ID: SV-223867r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-UT-000040](#)

Rule Title: IBM z/OS UNIX Telnet server Startup parameters must be properly specified.

Legacy ID: V-98441

Legacy ID: SV-107545

Vulnerability Discussion: The z/OS UNIX Telnet Server (i.e., otelnetd) provides interactive access to the z/OS UNIX shell. During the initialization process, startup parameters are read to define the characteristics of each otelnetd instance. Some of these parameters have an impact on system security. Failure to specify the appropriate command options could result in degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Check Content:

From the ISPF Command Shell enter:

ISHELL

Enter /etc/ for a pathname - you may need to issue a CD /etc/
select FILE NAME inetd.conf

If Option -D login is included on the otelnetd command, this is not a finding.

If Option -c 900 is included on the otelnetd command, this is not a finding.

NOTE: "900" indicates a session timeout value of "15" minutes and is currently the maximum value allowed.

Fix Text: Configure the startup parameters in the inetd.conf file for otelnetd to conform to the specifications below.

The otelnetd startup command includes the options -D login and -c 900, where:

-D login indicates that messages should be written to the syslogd facility for login and logout activity.

-c 900 indicates that the Telnet session should be terminated after "15" minutes of inactivity.

NOTE: "900" is the maximum value; any value between "1" and "900" is acceptable.

CCI: CCI-000366

Group ID (Vulid): V-223868

Group Title: SRG-OS-000228-GPOS-00088

Rule ID: SV-223868r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-UT-000050](#)

Rule Title: The IBM z/OS UNIX Telnet server warning banner must be properly specified.

Legacy ID: V-98443

Legacy ID: SV-107547

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.

Check Content:

From the ISPF Command Shell enter:

ISHELL

Enter /etc/ for a pathname - you may need to issue a CD /etc/
select FILE NAME inetd.conf

If Option -h is included on the otelnetd command, this is a finding.

Fix Text: Configure the startup parameters in the inetd.conf file for otelnetd to exclude option -h.

Note: -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-223869

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-223869r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-VT-000010](#)

Rule Title: IBM z/OS System datasets used to support the VTAM network must be properly secured.

Legacy ID: V-98445

Legacy ID: SV-107549

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:

Determine 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 RACF data set rules for all VTAM system data sets restrict access to only network systems programming staff, this is not a finding.

If RACF data set rules for all VTAM system data sets all READ access to auditors only, this is not a finding.

Fix Text: Configure RACF data set rules for all VTAM system data sets restrict access to only network systems programming staff. These data sets include libraries containing VTAM load modules and exit routines, and VTAM start options and definition statements.

Auditors may have READ access as documented by and approved by the ISSM.

The following sample RACF commands show proper definitions/permissions for VTAM datasets:

```
AD 'SYS1.VTAM.*.*' UACC(NONE) OWNER(SYS1) -  
AUDIT(SUCCESS(UPDATE) FAILURES(READ)) -  
DATA('IBM VTAM DS PROFILE: REF SRR PDI ZVTM0018')  
PE 'SYS1.VTAM.*.*' ID(<syspsmpl>) ACC(A)
```

```
AD 'SYS1.VTAMLIB.*.*' UACC(NONE) OWNER(SYS1) -  
AUDIT(SUCCESS(UPDATE) FAILURES(READ)) -  
DATA('IBM VTAM APF DS PROFILE: REF SRR PDI ZVTM0018')  
PE 'SYS1.VTAMLIB.*.*' ID(<syspsmpl>) ACC(A)
```

```
AD 'SYS1.VTAM.SISTCLIB.*.*' UACC(NONE) OWNER(SYS1) -  
AUDIT(SUCCESS(UPDATE) FAILURES(READ)) -  
DATA('IBM VTAM APF DS PROFILE: REF SRR PDI ZVTM0018')  
PE 'SYS1.VTAM.SISTCLIB.*.*' ID(<syspsmpl>) ACC(A)
```

```
AD 'SYS3.VTAM.*.*' UACC(NONE) OWNER(SYS3) -  
AUDIT(SUCCESS(UPDATE) FAILURES(READ)) -  
DATA('VTAM CUSTOMIZED DS: REF SRR PDI ZVTM0018')  
PE 'SYS3.VTAM.*.*' ID(<syspsmpl>) ACC(A)
```

```
AD 'SYS3.VTAMLIB.*.*' UACC(NONE) OWNER(SYS3) -  
AUDIT(SUCCESS(UPDATE) FAILURES(READ)) -  
DATA('IBM VTAM APF DS PROFILE: REF SRR PDI ZVTM0018')  
PE 'SYS3.VTAMLIB.*.*' ID(<syspsmpl>) ACC(A)
```

SETR GENERIC(DATASET) REFRESH

CCI: CCI-000213

CCI: CCI-001499

Group ID (Vulid): V-223870

Group Title: SRG-OS-000259-GPOS-00100

Rule ID: SV-223870r604139_rule

Severity: CAT II

Rule Version (STIG-ID): [RACF-VT-000020](#)

Rule Title: IBM z/OS VTAM USSTAB definitions must not be used for unsecured terminals.

Legacy ID: V-98447

Legacy ID: SV-107551

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.

Check Content:

Ask the system administrator to supply the following information:

- Documentation regarding terminal naming standards.
- Documentation of all procedures controlling terminal logons to the system.
- A complete list of all USS commands used by terminal users to log on to the system.
- Members and data set names containing USSTAB and LOGAPPL definitions of all terminals that can log on to the system (e.g., SYS1.VTAMLST).
- Members and data set names containing logon mode parameters.

If USSTAB definitions are only used for secure terminals (e.g., terminals that are locally attached to the host or connected to the host via secure leased lines), this is not a finding.

If USSTAB definitions are used for any unsecured terminals (e.g., dial up terminals or terminals attached to the Internet such as TN3270 or KNET 3270 emulation), this is a finding.

Fix Text: Configure USSTAB definitions to be only used for secure terminals.

Only terminals that are locally attached to the host or connected to the host via secure leased lines located in a secured area. Only authorized personnel may enter the area where secure terminals are located.

USSTAB or LOGAPPL definitions are used to control logon from secure terminals. These terminals can log on directly to any VTAM application (e.g., TSO, CICS, etc.) of their choice and bypass Session Manager services. Secure terminals are usually locally attached to the host or connected to the host via a private LAN without access to an external network. Only authorized personnel may enter the area where secure terminals are located.

CCI: CCI-001499

UNCLASSIFIED