

UNCLASSIFIED

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

z/OS WebsphereMQ for RACF STIG

Version: 7

Release: 1

15 Mar 2025

XSL Release 5/15/2012 Sort by: STIGID

Description:

Group ID (Vulid): V-224551

Group Title: ZWMQ0011

Rule ID: SV-7259r4_rule

Severity: CAT I

Rule Version (STIG-ID): ZWMQ0011

Rule Title: WebSphere MQ channel security must be implemented in accordance with security requirements.

Vulnerability Discussion: WebSphere MQ Channel security can be configured to provide authentication, message privacy, and message integrity between queue managers. Secure Sockets Layer (SSL) uses encryption techniques, digital signatures and digital certificates to provide message privacy, message integrity and mutual authentication between clients and servers.

Failure to properly secure a WebSphere MQ channel may lead to unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of some system services, applications, and customer data.

Documentable: YES

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECNK-1, ECNK-2

Check Content:

a) Create a report showing the WebSphere MQ channel definitions by submitting the JCL below. Add a job card and change the SSID value in the EXEC statement to your MQ SSID.

Note: This job must be run for each SSID.

```
//STEP1 EXEC PGM=CSQUTIL,PARM='SSID'
//STEPLIB DD DSN=CSQ700.SCSQAUTH,DISP=SHR
// DD DSN=CSQ700.SCSQANLE,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
COMMAND
//CSQUCMD DD *
DISPLAY SECURITY ALL
DISPLAY QUEUE(*) ALL
DISPLAY NAMELIST(*) ALL
DISPLAY PROCESS(*) ALL
DISPLAY CHANNEL(*) ALL
DISPLAY QMGR DEADQ
DISPLAY QMGR SSLKEYR
```

Below is a sample of the WebSphere MQ channel definition needed to remediate this STIG.

b) For each WebSphere MQ channel configured to communicate with servers using WebSphere MQ, review the ssid report(s) and perform the following steps:

1. Verify that each WebSphere MQ channel is using SSL by checking for the SSLCIPH parameter, which specifies a cipher specification:

```
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
```

(Both ends of the channel must specify the same cipher specification.)

2. Repeat these steps for each queue manager ssid identified.

c) For each queue manager ssid identified, if the SSLCIPH parameter, on both sides of each WebSphere MQ channel, specifies the above in b. there is NO FINDING.

d) If the communication lines are controlled by a VPN and are not available in the clear at any point outside the enclave, than this is acceptable and can override the requirement to use SSL. If this is true, there is NO FINDING.

e) For each queue manager ssid identified , if either side of each WebSphere MQ channel specifies a cipher specification other than specified in b , this is a FINDING unless the communication lines are controlled by a VPN and traffic is not available in the clear at any point outside of the enclave.

For each queue manager ssid identified, if either side of each WebSphere MQ channel specifies a cipher specification other than DES or DES3, and the communication lines are not controlled by a VPN, this is a FINDING.

Fix Text: The system programmer and the IAO will review the WebSphere MQ Screen interface invoked by the REXX CSQOREXX. Reviewing the channel s SSLCIPH setting.

Display the channel properties and look for the "SSL Cipher Specification" value.

Ensure that a FIPS 140-2 compliant value is shown.

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

Note that both ends of the channel must specify the same cipher specification.

Repeat these steps for each queue manager ssid identified.

CCI: CCI-000068

CCI: CCI-002421

CCI: CCI-002423

CCI: CCI-002450

Group ID (Vulid): V-224552

Group Title: ZWMQ0012

Rule ID: SV-7283r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0012

Rule Title: WebSphere MQ channel security is not implemented in accordance with security requirements.

Vulnerability Discussion: WebSphere MQ channel security can be configured to provide authentication, message privacy, and message integrity between queue managers. WebSphere MQ channels use SSL encryption techniques, digital signatures and digital certificates to provide message privacy, message integrity and mutual authentication between clients and servers.

Failure to properly secure a WebSphere MQ channel may lead to unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of some system services, applications, and customer data.

Responsibility: Information Assurance Officer

IA Controls: DCCS-1, DCCS-2

Check Content:

a) Create a report showing the WebSphere MQ channel definitions by submitting the JCL below. Add a job card and change the SSID value in the EXEC statement to your MQ SSID.

Note: This job must be run for each SSID.

```
//STEP1 EXEC PGM=CSQUTIL,PARM='SSID'
//STEPLIB DD DSN=CSQ700.SCSQAUTH,DISP=SHR
// DD DSN=CSQ700.SCSQANLE,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
COMMAND
//CSQUCMD DD *
DISPLAY SECURITY ALL
DISPLAY QUEUE(*) ALL
DISPLAY NAMELIST(*) ALL
DISPLAY PROCESS(*) ALL
DISPLAY CHANNEL(*) ALL
DISPLAY QMGR DEADQ
DISPLAY QMGR SSLKEYR
```

b) If the site is running MQSeries 5.2 or below, this is NOT APPLICABLE.

The MQSeries release number can be found in message CSQU000I.

CSQU000I CSQUTIL IBM MQSeries for Z/OS - V5.2

CSQU001I CSQUTIL Queue Manager Utility - 2000-05-09 09:06:48

c) For each WebSphere MQ 5.3 and above, review the ssid report(s) and perform these steps for each queue manager ssid identified:

d) Review the output from step a.

e) Verify that each WebSphere MQ 5.3 queue manager is using a digital certificate by reviewing the SSLKEYR parameter to ensure that a keyring is identified. i.e. SSLKEYR(sslkeyring-id)

- f) If the SSLKEYR parameter contains a value of sslkeyring-id, there is NO FINDING.
- g) If the SSLKEYR parameter does not contain a value of sslkeyring-id, there is a FINDING.
- h) Issue the following RACF commands, where ssidCHIN is the lid for the WebSphere MQ Channel Initiator's userid and sslkeyring-id is obtained from the above action:

RACDCERT ID(ssidCHIN) LISTRING(sslkeyring-id)

NOTE: The sslkeyring-id is case sensitive.

The output will contain columns for Certificate Label Name and Cert Owner. Find the Cert Owner of ID(ssidCHIN). Use the Certificate Label Name for ID(ssidCHIN) in the following command:

RACDCERT ID(ssidCHIN)
LIST(LABEL(Certificate Label Name))

NOTE: The Certificate Label Name is case sensitive.

Review the Issuer's Name field in the resulting output for information of any of the following:

OU=PKI.OU=DoD.O=U.S. Government.C=US
OU=ECA.O=U.S. Government.C=US

- i) Repeat these steps for each queue manager ssid identified.
- j) If OU= equals either of the above in item h) there is no finding for the OU=.

Check Content:

- a) Refer to the following report produced by the z/OS Data Collection:

- MQRPT(ssid)

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier). To determine which Release of WebSphere MQ, review ssid reports for message CSQU000I.

Collect the following Information for Websphere MQ queue manager

- If a WebSphere MQ queue manager communicates with a MQSeries queue manager, provide the WebSphere MQ queue manager and channel names used to connect with MQSeries.
- If any WebSphere MQ channels are used to communicate within the enclave, provide a list of channels and provide documentation regarding the sensitivity of the information on the channel.
- b) Review the ssid report(s) and perform the following steps:
 - 1) Find the DISPLAY QMGR SSLKEYR command to locate the start of the Queue Manager definitions.
 - 2) Verify that each WebSphere MQ 5.3 queue manager is using a digital certificate by reviewing the

SSLKEYR parameter to ensure that a keyring is identified. i.e. SSLKEYR(sslkeyring-id)

3) Issue the following RACF commands, where ssidCHIN is the logonid for the WebSphere MQ Channel Initiator's userid and sslkeyring-id is obtained from the above action:

RACDCERT ID(ssidCHIN) LISTRING(sslkeyring-id)

NOTE: The sslkeyring-id is case sensitive.

The output will contain columns for Certificate Label Name and Cert Owner. Find the Cert Owner of ID(ssidCHIN). Use the Certificate Label Name for ID(ssidCHIN) in the following command:

RACDCERT ID(ssidCHIN) LIST(LABEL(Certificate Label Name))

NOTE: The Certificate Label Name is case sensitive.

Review the Issuer's Name field in the resulting output for information of any of the following:

OU=PKI.OU=DoD.O=U.S. Government.C=US

OU=ECA.O=U.S. Government.C=US

- 4) Repeat these steps for each queue manager ssid identified.
- c) If all of the items in (b) above are true, there is NO FINDING.
- d) If any of the items in (b) above are untrue, this is a FINDING.

Check Content:

a) Refer to the following report produced by the z/OS Data Collection:

- MQRPT(ssid)

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier). To determine which Release of WebSphere MQ, review ssid reports for message CSQU000I.

Collect the following Information for Websphere MQ queue manager

- If a WebSphere MQ queue manager communicates with a MQSeries queue manager, provide the WebSphere MQ queue manager and channel names used to connect with MQSeries.
- If any WebSphere MQ channels are used to communicate within the enclave, provide a list of channels and provide documentation regarding the sensitivity of the information on the channel.

b) Review the ssid report(s) and perform the following steps:

- 1) Find the DISPLAY QMGR SSLKEYR command to locate the start of the Queue Manager definitions.
- 2) Verify that each WebSphere MQ 5.3 queue manager is using a digital certificate by reviewing the SSLKEYR parameter to ensure that a keyring is identified. i.e. SSLKEYR(sslkeyring-id)
- 3) Issue the following TSS commands, where ssidCHIN is the Acid for the WebSphere MQ Channel Initiator's userid and sslkeyring-id is obtained from the above action:

TSS LIST(ssidCHIN) KEYRING(sslkeyring-id)

NOTE: The sslkeyring-id is case sensitive.

In the output find the DIGICERT field for ACID(ssidCHIN). Use this DIGICERT in the following command:

TSS LIST(ssidCHIN) DIGICERT(digicert)

NOTE: The digicert is case sensitive.

Review the ISSUER DISTINGUISHED NAME field in the resulting output for information of any of the following:

OU=PKI.OU=DoD.O=U.S. Government.C=US

OU=ECA.O=U.S. Government.C=US

- 4) Repeat these steps for each queue manager ssid identified.
- c) If the all of the items in (b) above are true, there is NO FINDING.
- d) If any of the items in (b) above are untrue, this is a FINDING.

Fix Text: Refer to the following report produced by the z/OS Data Collection:

- MQSRPT(ssid)

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) Find the DISPLAY QMGR SSLKEYR command to locate the start of the Queue Manager definitions.
- 2) Verify that each WebSphere MQ queue manager is using a digital certificate by reviewing the SSLKEYR parameter to ensure that a keyring is identified. i.e. SSLKEYR(sslkeyring-id)
- 3) Issue the following RACF commands, where ssidCHIN is the lid for the WebSphere MQ Channel Initiator s userid and sslkeyring-id is obtain from the above action:

RACDCERT ID(ssidCHIN) LISTRING(sslkeyring-id)

NOTE: The sslkeyring-id is case sensitive.

The output will contain columns for Certificate Label Name and Cert Owner. Find the Cert Owner of ID(ssidCHIN). Use the Certificate Label Name for ID(ssidCHIN) in the following command:

RACDCERT ID(ssidCHIN) LIST(LABEL(Certificate Label Name))

NOTE: The Certificate Label Name is case sensitive.

Review the Issuer s Name field in the resulting output for information of any of the following:

OU=PKI.OU=DoD.O=U.S. Government.C=US

OU=ECA.O=U.S. Government.C=US

- 4) Repeat these steps for each queue manager ssid identified.

To implement the requirements stated above, the following two items are provided which attempt to assist with (1)

Technical "how to" information and (2) A DISA Point of contact for obtaining SSL certificates for CSD WebSphere MQ channels:

1. Review the information available on setting up SSL, Keyrings, and Digital Certificates in the RACF Security Administrator's Guide as well as the WebSphere MQ Security manual. Also review the information contained in the documentation provided as part of the install package from the DISA SSO Resource Management Factory (formerly Software Factory).
2. For information on obtaining an SSL certificate in the DISA CSD environment, send email inquiry to disaraoperations@disa.mil for more info.

Fix Text: Refer to the following report produced by the z/OS Data Collection:

- MQSRPT(ssid)

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) Find the DISPLAY QMGR SSLKEYR command to locate the start of the Queue Manager definitions.
- 2) Verify that each WebSphere MQ queue manager is using a digital certificate by reviewing the SSLKEYR parameter to ensure that a keyring is identified. i.e. SSLKEYR(sslkeyring-id)
- 3) Issue the following ACF2 command, where ssidCHIN is the lid for the WebSphere MQ Channel Initiator s userid and sslkeyring-id is obtain from the above action:

LIST ssidCHIN PROFILE(CERTDATA, KEYRING)

The output will contain information on the CERTDATA and KEYRING records for the user. Find the CERTDATA entry that has a Key ring name field with sslkeyring-id. Review the ISSUERDN field for this CERTDATA record for the following:

OU=PKI.OU=DoD.O=U.S. Government.C=US
OU=ECA.O=U.S. Government.C=US

NOTE: The Certificate Label Name is case sensitive.

Review the Issuer s Name field in the resulting output for information of any of the following:

OU=PKI.OU=DoD.O=U.S. Government.C=US
OU=ECA.O=U.S. Government.C=US

- 4) Repeat these steps for each queue manager ssid identified.

To implement the requirements stated above, the following two items are provided which attempt to assist with (1) Technical "how to" information and (2) A DISA Point of contact for obtaining SSL certificates for CSD WebSphere MQ channels:

1. Review the information available on setting up SSL, Keyrings, and Digital Certificates in the CA-ACF2 Security for z/OS Administrators Guide as well as the WebSphere MQ Security manual. Also review the information contained in the documentation provided as part of the install package from the DISA SSO Resource Management Factory (formerly Software Factory).
2. For information on obtaining an SSL certificate in the DISA CSD environment, send email inquiry to

disaraoperations@disa.mil for more info.

Fix Text: Refer to the following report produced by the z/OS Data Collection:

- MQSRPT(ssid)

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) Find the DISPLAY QMGR SSLKEYR command to locate the start of the Queue Manager definitions.
- 2) Verify that each WebSphere MQ queue manager is using a digital certificate by reviewing the SSLKEYR parameter to ensure that a keyring is identified. i.e. SSLKEYR(sslkeyring-id)
- 3) Issue the following TSS commands, where ssidCHIN is the lid for the WebSphere MQ Channel Initiator s userid and sslkeyring-id is obtain from the above action:

TSS LIST(ssidCHIN) KEYRING(sslkeyring-id)

NOTE: The sslkeyring-id is case sensitive.

In the output find the DIGICERT field for ACID(ssidCHIN). Use this DIGICERT in the following command:

TSS LIST(ssidCHIN) DIGICERT(digicert)

NOTE: The Certificate Label Name is case sensitive.

Review the Issuer s Name field in the resulting output for information of any of the following:

OU=PKI.OU=DoD.O=U.S. Governmemt.C=US

OU=ECA.O=U.S. Government.C=US

- 4) Repeat these steps for each queue manager ssid identified.

To implement the requirements stated above, the following two items are provided which attempt to assist with (1) Technical "how to" information and (2) A DISA Point of contact for obtaining SSL certificates for CSD WebSphere MQ channels:

1. Review the information available on setting up SSL, Keyrings, and Digital Certificates in the CA TSS Cookbook regarding usage of the TSS commands to administer PKI Certificates as well as the WebSphere MQ Security manual. Also review the information contained in the documentation provided as part of the install package from the DISA SSO Resource Management Factory (formerly Software Factory).

2. For information on obtaining an SSL certificate in the DISA CSD environment, send email inquiry to disaraoperations@disa.mil for more info.

CCI: CCI-002470

Group ID (Vulid): V-224553

Group Title: ZWMQ0014

Rule ID: SV-41848r5_rule

Severity: CAT II**Rule Version (STIG-ID):** ZWMQ0014**Rule Title:** Production WebSphere MQ Remotes must utilize Certified Name Filters (CNF)

Vulnerability Discussion: IBM Websphere MQ can use a user ID associated with an ACP certificate as a channel user ID. When an entity at one end of an SSL channel receives a certificate from a remote connection, the entity asks The ACP if there is a user ID associated with that certificate. The entity uses that user ID as the channel user ID. If there is no user ID associated with the certificate, the entity uses the user ID under which the channel initiator is running. Without a validly defined Certificate Name Filter for the entity IBM Websphere MQ will set the channel user ID to the default.

Responsibility: N/A**IAControls:** N/A**Check Content:**

a) Create a report listing the WebSphere MQ remote queues by submitting the JCL below. Add a job card and change the SSID value in the EXEC statement to your MQ SSID.

Note: This job must be run for each SSID.

```
//STEP1 EXEC PGM=CSQUTIL,PARM='SSID'
//STEPLIB DD DSN=CSQ700.SCSQAUT,DISP=SHR
// DD DSN=CSQ700.SCSQANLE,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
COMMAND
//CSQUCMD DD *
DISPLAY QUEUE(*) TYPE(QREMOTE) ALL
/*
```

b) For each WebSphere MQ 5.3 and above, review the ssid report(s) and perform the following steps.

(The MQSeries release number can be found in message CSQU000I from running the CSQUTIL in step a) above.
 CSQU000I CSQUTIL IBM MQSeries for Z/OS - V5.2
 CSQU001I CSQUTIL Queue Manager Utility - 2000-05-09 09:06:48)

c) From Administrator main menu, select Security Server Reports and press Enter.

d) Select General Resource Profile, option 4 and press Enter.

e) Tab down to the Class field, enter MQQUEUE and press Enter.

f) Find any remote queue names from the report in step a) above on the screen and enter LR next to the queue name.

g) Press ENTER

- h) Note down all the users in the access list.
- i) List information about the certificates for each specific userid in step h) using the RACDCERT command.
- j) Verify the certificates are valid per qualifications in STIG ITNT0040.
- k) If one or more users are found with valid certificates, for each remote queue from step a) above, there is NO FINDING.
- l). If no users are found with accurate filters for any of the remote queues, this is a FINDING.
- m). If a spreadsheet is not maintained containing a list of all production Websphere MQ remote queues with associated individual USERIDS with corresponding valid Certified Name filters and reviewed annually, this is a FINDING.

Fix Text: The responsible MQ System programmer(s) shall create and maintain a spread sheet that contains a list of all Production WebSphere MQ Remotes, associated individual USERIDs with corresponding valid Certified Name Filters (CNF). This documentation will be reviewed and validated annually by responsible MQ System programmer(s) and forwarded for approval by the ISSM.

The ISSO will define the associated USERIDs, the CNF, and grant the minimal need to know access, by granting only the required resources and Commands for each USERID in the ACP. See IBM WebSphere MQ Security manual for details on defining CNF for WebSphere MQ.

Generic access shall not be granted such as resource permission at the SSID. MQ resource level.

CCI: CCI-000366

CCI: CCI-001133

Group ID (Vulid): V-224554

Group Title: ZWMQ0020

Rule ID: SV-3903r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0020

Rule Title: User timeout parameter values for WebSphere MQ queue managers are not specified in accordance with security requirements.

Vulnerability Discussion: Users signed on to a WebSphere MQ queue manager could leave their terminals unattended for long periods of time. This may allow unauthorized individuals to gain access to WebSphere MQ resources and application data. This exposure could compromise the availability, integrity, and confidentiality of some system services and application data.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, ECTM-1, ECTM-2

Check Content:

a) Create a report showing the WebSphere MQ channel definitions by submitting the JCL below. Add a job card and change the SSID value in the EXEC statement to your MQ SSID.

Note: This job must be run for each SSID.

```
//STEP1 EXEC PGM=CSQUTIL,PARM='SSID'
//STEPLIB DD DSN=CSQ700.SCSQAUTH,DISP=SHR
// DD DSN=CSQ700.SCSQANLE,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
COMMAND
//CSQUCMD DD *
DISPLAY SECURITY ALL
DISPLAY QUEUE(*) ALL
DISPLAY NAMELIST(*) ALL
DISPLAY PROCESS(*) ALL
DISPLAY CHANNEL(*) ALL
DISPLAY QMGR DEADQ
DISPLAY QMGR SSLKEYR
```

b) Review messages CSQH015I and CSQH016I:

```
12.36.22 STC01960 CSQH015I !MQ19 Security timeout = 15 minutes
12.36.22 STC01960 CSQH016I !MQ19 Security interval = 5 minutes
```

The Z/OS STIG standard value for interval is: INTERVAL(5).

The Z/OS STIG standard value for timeout is: TIMEOUT(15)

c) If the timeout value equals 15 minutes, there is NO FINDING.
If the interval value equals 5 minutes, there is NO FINDING.

d) If the timeout value does not equal 15 minutes, this is a FINDING
If the interval value is not equal to 5 minutes, this is a FINDING

Repeat steps (a) thru (d) for each queue manager ssid.

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

Fix Text: Review the WebSphere MQ System Setup Guide and the information on the ALTER SECURITY command in the WebSphere MQ Script (MQSC) Command Reference.

Ensure the values for the TIMEOUT and INTERVAL parameters are specified in accordance with security requirements.

CCI: CCI-001133

Group ID (Vulid): V-224555

Group Title: ZWMQ0030

Rule ID: SV-7526r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0030

Rule Title: WebSphere MQ started tasks are not defined in accordance with the proper security requirements.

Vulnerability Discussion: Started tasks are used to execute WebSphere MQ queue manager services. Improperly defined WebSphere MQ started tasks may result in inappropriate access to application resources and the loss of accountability. This exposure could compromise the availability of some system services and application data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

a) Work with the systems programmer to identify the names of all MQSeries/WebSphere MQ started tasks.

b) Review MQSeries/WebSphere MQ started tasks to ensure that:

1. Each MQ started task (ssidMSTR and ssidCHIN) is associated with a unique userid.
2. All MQ started tasks (ssidMSTR and ssidCHIN) are defined to the STARTED resource class.
3. All MQ started tasks (ssidMSTR and ssidCHIN) userid are defined as a PROTECTED.

Using Vanguard Analyzer:

1. From the main Menu, select 3 (Online Displays), press <ENTER>.
2. Select 4 (Started Procedures Analysis) and press <ENTER>.

Review the Procname and USERID columns associated with each MQSeries/WebSphere MQ started task identified in step a).

Using Vanguard Administrator:

1. From the main menu, type 3 (Security Server Reports), press <ENTER>.
2. Type 1 (User Profiles), press <Enter>.
3. Tab down to the PROTECTED field, type Y and press <ENTER>.
4. All PROTECTED userids will be displayed.

b) For each MQ started task name, if the userid contained in the Userid column of the Analyzer report is unique (i.e. is not associated with any other started task name), there is NO FINDING.

c) If the name of each MQ started task is displayed in the Procname column of the Analyzer report (e.g. defined to the STARTED resource class), there is NO FINDING.

d) Using the Administrator Protected Userid Report , if all MQ started tasks (identified in the Analyzer report) appear in the Userid column, there is NO FINDING.

e) For each MQ started task name, if the userid contained in the Userid column of the Analyzer report is not unique (i.e. is associated with other started task names), this is a FINDING

f) If the name of any MQ started task is not displayed in the Procname column of the Analyzer report (e.g. not defined to the STARTED resource class), this is a FINDING.

g) Using the Administrator Protected Userid Report , if a MQ started task userid (identified in the Analyzer report) does not appear in the Userid column, this is a FINDING

Fix Text: Each queue manager started task procedure xxxxMSTR and distributed queuing started task procedure xxxxCHIN will have a matching profile defined to the STARTED resource class. Create a corresponding userid for each started task. The STC userids will be defined as PROTECTED userids. Queue manager and channel initiator started tasks will not be defined with the TRUSTED attribute.

The following sample contains commands to properly define the required Started Procs:

Note that this example uses "qmq1" as the value for ssid.

```
AU qmq1mstr NAME('STC, MQSERIES') NOPASS DFLTGRP(STC) OWNER(STC) DATA('MQSERIES
QUEUE MANAGER PROC')
```

```
AU qmq1chin NAME('STC, MQSERIES') NOPASSDFLTGRP(STC) OWNER(STC) DATA('MQSERIES
DISTRIBUTED QUEUING CHANNEL INIT PROC')
```

```
RDEF STARTED qmq1mstr.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MAP
qmq1mstr PROC TO qmq1mstr USERID') STDATA(USER(=MEMBER) GROUP(STC) TRACE(YES))
```

```
RDEF STARTED qmq1chin.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MAP
qmq1mstr PROC TO qmq1chin USERID') STDATA(USER(=MEMBER) GROUP(STC) TRACE(YES))
```

```
SETR RACL(STARTED) REFRESH
```

CCI: CCI-000764

Group ID (Vulid): V-224556

Group Title: ZWMQ0040

Rule ID: SV-3905r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0040

Rule Title: WebSphere MQ all update and alter access to MQSeries/WebSphere MQ product and system data sets are not properly restricted

Vulnerability Discussion: MVS data sets provide the configuration, operational, and executable properties of WebSphere MQ. Some data sets are responsible for the security implementation of WebSphere MQ. Failure to properly protect these data sets may lead to unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECCD-1, ECCD-2

Check Content:

a) Consult with the MQSeries systems programmer to identify the names of the MQSeries system data sets, log data sets and archive datasets that protect MQSeries data.

b) Ensure RACF data sets rules for MQSeries/WebSphere MQ system data sets (e.g., SYS2.MQM.***) restrict access as follows:

___ READ access to data sets referenced by the following DDnames is restricted to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, and system programming personnel. All access to these data sets is logged.

DDname Procedure Description

CSQINP1 ssidMSTR Input parameters

CSQINP2 ssidMSTR Input parameters

CSQXLIB ssidCHIN User exit library

NOTE: UPDATE and/or ALTER access to these data sets is restricted to MQSeries/WebSphere

Using Administrator:

1. From the main menu, go to the Dataset Profile Reports menu by typing 3;3 and press <ENTER>.
2. Tab down to the Data Set row and over-type the * with the names of each dataset identified in step a).
3. Review the universal access, access list and audit attributes for each profile that protects datasets identified in step a).

For dataset profiles that protect resources identified in the above DDname statements:

1. If MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, and system programming personnel have READ access, there is NO FINDING.
2. If MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, and system programming personnel have UPDATE and/or ALTER access, there is a FINDING.

3. If audit ALL(READ) is specified, there is NO FINDING

4. If audit ALL(READ) is not specified, there is a FINDING.

___ UPDATE and/or ALTER access to data sets referenced by the following DDnames is restricted to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, and systems programming personnel. All UPDATE and ALTER access to these data sets is logged.

DDname Procedure Description

CSQPxxxx ssidMSTR Page data sets

BSDSx ssidMSTR Bootstrap data sets

CSQOUTx ssidMSTR SYSOUT data sets

CSQSNAP ssidMSTR DUMP data set

(See note) ssidMSTR Log data sets

NOTE: To determine the log data set names, review the JESMSG LG file of the ssidMSTR active task(s). Find CSQJ001I messages to obtain DSNs.

For dataset profiles that protect resources identified in the above DDname statements:

5. If MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators and system programming personnel have UPDATE and/or ALTER access, there is NO FINDING.

6. If any users other than MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators and system programming personnel have an access level greater than UPDATE, there is a FINDING.

7. If all UPDATE and ALTER access to these datasets is being logged, there is NO FINDING

8. If all UPDATE and ALTER access to these datasets is not being logged, there is a FINDING.

___ ALTER access to archive data sets is restricted to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrator, and system programming personnel. All ALTER access to these data sets is logged.

NOTE: To determine the archive data sets names, review the JESMSG LG file of the ssidMSTR active task(s). Find the CSQY122I message to obtain the ARCPRFX1 and ARCPRFX2 DSN HLQs.

9. If ALTER access to archive data sets is restricted to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrator, and system programming personnel, there is NO FINDING.

10. If ALTER access to archive data sets is not restricted to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrator, and system programming personnel, there is a FINDING.

11. If all ALTER accesses to archive data sets is being logged, there is NO FINDING.

12. If all ALTER access to archive data sets is not being logged, there is a FINDING.

13. Except for the specific data set requirements just mentioned, if UPDATE and/or ALTER access to all other MQSeries/WebSphere MQ system datasets is restricted to the MQSeries/WebSphere MQ administrator and systems programming personnel, there is NO FINDING.

14. Except for the specific data set requirements just mentioned, if UPDATE and/or ALTER access to all other MQSeries/WebSphere MQ system datasets is not restricted to the MQSeries/WebSphere MQ administrator and systems programming personnel, there is a FINDING.

c) If all the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

Fix Text: The systems programmer will have the IAO ensure that all update and alter access to MQSeries/WebSphere MQ product and system data sets are restricted to WebSphere MQ administrators, systems programmers, and MQSeries/WebSphere MQ started tasks.

The installation requires that the following data sets be APF authorized.

hlqual.SCSQAUTH
hlqual.SCSQLINK
hlqual.SCSQANLx
hlqual.SCSQSNL
hlqual.SCSQMVR1
hlqual.SCSQMVR2

(2) Read access to data sets referenced by the CSQINP1, CSQINP2, and CSQXLIB DDs in the queue manager s procedure will be restricted to the queue manager userid, WebSphere MQ administrator, and systems programming personnel. Log all access to these data sets.

(3) Write and allocate access to data set profiles protecting all page sets, logs, bootstrap data sets (BSDS), and data sets referenced by the CSQOUTX and CSQSNAP DDs in the queue manager s procedure will be restricted to the queue manager userid, WebSphere MQ administrator, and systems programming personnel. Log all write and allocate access to these data sets.

(5) Allocate access to all archive data sets in the queue manager s procedure will be restricted to the queue manager userid, WebSphere MQ administrator, and systems programming personnel. Log all allocate access to these data sets.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

Group ID (Vulid): V-224557

Group Title: ZWMQ0049

Rule ID: SV-7534r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0049

Rule Title: WebSphere MQ resource classes are not properly activated for security checking by the ACP.

Vulnerability Discussion: WebSphere MQ resources allow for the control of administrator functions, connections, commands, queues, processes, and namelists. Some resources provide the ability to disable or bypass security checking. Failure to ensure the classes have been made ACTIVE under RACF will prevent RACF from enforcing security rules. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Use Analyzer to display active classes.

1. From the Analyzer main Menu, select 3 (Online Displays), press <ENTER>
2. Select 7 (SETROPTS Analysis) and press <ENTER>
3. Tab down and type an S next to Audit for CDT Classes , press <ENTER>
4. Resource class names are displayed in the Class column, the status of each resource class name (inactive/active) is displayed in the Status column.
5. Press PF8 to find each class name documented in b) below.

b) Ensure that the following MQ Series resource classes are active below V7.0.0

MQADMIN
 GMQADMIN
 MQCONN
 MQCMDS
 MQQUEUE
 GMQUEUE
 MQPROC
 GMQPROC
 MQNLIST
 GMQNLIST

For V7.0.0 and above these classes must be active:

GMXADMIN
 GMXNLIST
 GMXPROC

GMXQUEUE
 GMXTOPIC
 MXADMIN
 MXNLIST
 MXPROC
 MXQUEUE
 MXTOPIC

NOTE: If the MQADMIN resource class is not active, no security checking is performed.

c) If all of the resource classes above are ACTIVE (e.g. active is displayed in the status column), there is NO FINDING.

d) If any resource classes above are INACTIVE (e.g. inactive is displayed in the status column), this is a FINDING.

—

Fix Text: The IAO will ensure that all WebSphere MQ resources are active and properly defined.

Ensure the following WebSphere MQ resource classes are active:

GMQADMIN
 GMQNLIST
 GMQPROC
 GMQQUEUE
 MQADMIN
 MQCMDS
 MQCONN
 MQNLIST
 MQPROC
 MQQUEUE

For V7.0.0 and above:

GMXADMIN
 GMXNLIST
 GMXPROC
 GMXQUEUE
 GMXTOPIC
 MXADMIN
 MXNLIST
 MXPROC
 MXQUEUE
 MXTOPIC

NOTE: If both MQADMIN and MXADMIN resource classes are not active, no security checking is performed.

The follow sample contains commands to active the required classes:

SETR CLASSACT(MQADMIN MQCMDS MQCONN)
 SETR CLASSACT(MQNLIST MQPROC MQQUEUE)
 SETR CLASSACT(MXADMIN MXNLIST MXPROC MXQUEUE)

CCI: CCI-000213

CCI: CCI-002358

Group ID (Valid): V-224558

Group Title: ZWMQ0051

Rule ID: SV-7538r2_rule

Severity: CAT I

Rule Version (STIG-ID): ZWMQ0051

Rule Title: Security Switches

Vulnerability Discussion: WebSphere MQ resources allow for the control of administrator functions, connections, commands, queues, processes, and namelists. Some resources provide the ability to disable or bypass security checking. Failure to properly protect WebSphere MQ resources may result in unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Create a report showing the WebSphere MQ channel definitions by submitting the JCL below. Add a job card and change the SSID value in the EXEC statement to your MQ SSID.

Note: This job must be run for each SSID.

```
//STEP1 EXEC PGM=CSQUTIL,PARM='SSID'
//STEPLIB DD DSN=CSQ700.SCSQAUTH,DISP=SHR
// DD DSN=CSQ700.SCSQANLE,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
COMMAND
//CSQUCMD DD *
DISPLAY SECURITY ALL
DISPLAY QUEUE(*) ALL
DISPLAY NAMELIST(*) ALL
DISPLAY PROCESS(*) ALL
DISPLAY CHANNEL(*) ALL
DISPLAY QMGR DEADQ
DISPLAY QMGR SSLKEYR
```

b) Review the Security switches. If all of the following switches specify ON, there is NO FINDING.

SUBSYSTEM CONNECTION COMMAND CONTEXT ALTERNATE USER PROCESS NAMELIST QUEUE COMMAND RESOURCES

For example:

```
10.05.01 STC01960 CSQH030I !MQ19 Security switches ...
10.05.01 STC01960 CSQH034I !MQ19 SUBSYSTEM: ON,
10.05.01 STC01960 CSQH031I !MQ19 CONNECTION: ON,
10.05.01 STC01960 CSQH034I !MQ19 COMMAND: ON,
10.05.01 STC01960 CSQH031I !MQ19 CONTEXT: ON,
10.05.01 STC01960 CSQH034I !MQ19 ALTERNATE USER: ON,
10.05.01 STC01960 CSQH034I !MQ19 PROCESS: ON,
10.05.01 STC01960 CSQH034I !MQ19 NAMELIST: ON,
10.05.01 STC01960 CSQH034I !MQ19 QUEUE: ON,
10.05.01 STC01960 CSQH031I !MQ19 COMMAND RESOURCES: ON,
```

c) If the SUBSYSTEM switch is OFF, this is a FINDING with a severity of Category I.

d) If any of the other above switches specify OFF (other than the exception mentioned below), this is a FINDING, downgrade the severity to a Category II.

e) If the COMMAND RESOURCE Security switch specifies OFF, there is NO FINDING.

NOTE: At the discretion of the IAO, COMMAND RESOURCE Security switch may specify OFF, by defining ssid.NO.CMD.RESC.CHECKS in the MQADMIN resource class.

Fix Text: Switch profiles are special MQSeries/WebSphere MQ profiles that are used to turn on/off security checking for a type of resource. Due to the security exposure this creates, no profiles with the first two qualifiers of ssid.NO will be defined to the MQADMIN class, with one exception. Due to the fact that (1) all sensitive MQSeries/WebSphere MQ commands are restricted to queue managers, channel initiators, and designated systems personnel, and (2) no command resource checking is performed on DISPLAY commands, at the discretion of the IAO a ssid.NO.CMD.RESC.CHECKS switch profile may be defined to the MQADMIN class.

1. Identify if any switch profiles exist using the sample search command:

```
SR CLASS(MQADMIN) NOMASK FILTER(*.NO.**)
```

2. Use the "RDEL MQADMIN <SwitchProfileName>" to remove the profile and follow up with a "SETR RACL(MQADMIN) REF"

3. An additional refresh to an active WebSphere MQ Queue Manager may be required. A sample is shown below using the value QMD1 as the Queue Manager name.

From the Console:

>QMD1 REFRESH SECURITY(*)

CCI: CCI-000213

Group ID (Vulid): V-224559

Group Title: ZWMQ0052

Rule ID: SV-7541r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0052

Rule Title: Connection Resources

Vulnerability Discussion: WebSphere MQ resources allow for the control of administrator functions, connections, commands, queues, processes, and namelists. Some resources provide the ability to disable or bypass security checking. Failure to properly protect WebSphere MQ resources may result in unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following reports produced by the RACF Data Collection:

- SENSITIVE.RPT(MQCONN)

b) Review the following connection resources defined to the MQCONN resource class:

Resource	Authorized Users
ssid.BATCH	TSO and batch job userids
ssid.CICS	CICS region userids
ssid.IMS	IMS region userids
ssid.CHIN	Channel initiator userids

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

c) For all connection resources defined to the MQCONN resource class, ensure the following items are in effect:

NOTE: If you do not have a resource profile defined for a particular security check, and a user issues a request that would involve making that check, MQSeries/WebSphere MQ denies access.

- 1) Resource profiles are defined with a UACC(NONE).
- 2) Access authorization to these connections restricts access to the appropriate users as indicated in (b).
- 3) All access is logged, e.g., ALL(READ).

- d) If all of the items in (c) are true, there is NO FINDING.
- e) If any item in (c) is untrue, this is a FINDING.

Fix Text: Review the following connection resources defined to the MQCONN resource class:

Resource	Authorized Users
ssid.BATCH	TSO and batch job userids
ssid.CICS	CICS region userids
ssid.IMS	IMS region userids
ssid.CHIN	Channel initiator userids

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

- c) For all connection resources defined to the MQCONN resource class, ensure the following items are in effect:

NOTE: If you do not have a resource profile defined for a particular security check, and a user issues a request that would involve making that check, MQSeries/WebSphere MQ denies access.

- 1) Resource profiles are defined with a UACC(NONE).
- 2) Access authorization to these connections restricts access to the appropriate users as indicated in (b).
- 3) All access is logged, e.g., ALL(READ).

A set of sample commands are provided below to implement the minimum profiles necessary for proper security. Note that the IMS and/or CICS profiles can be omitted if those products do not run on the target system.

```
/* THE FOLLOWING PROFILE FORCES GRANULAR PROFILES DEFINITIONS */
RDEF MQCONN ** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQCONN DENY-BY-DEFAULT PROFILE')
```

```
RDEF MQCONN <ssid>.BATCH UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
DATA('REQUIRED FOR ZWMQ0052')
PE <ssid>.BATCH CL(MQCONN) ID(<applicableTSO&batchUsers>)
```

```
RDEF MQCONN <ssid>.CICS UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('REQUIRED
FOR ZWMQ0052')
PE <ssid>.CICS CL(MQCONN) ID(<CICSRegionUserids>)
```

```
RDEF MQCONN <ssid>.IMS UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('REQUIRED
FOR ZWMQ0052')
PE <ssid>.IMS CL(MQCONN) ID(<IMSRegionUserids>)
```

```
RDEF MQCONN <ssid>.CHIN UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('REQUIRED
FOR ZWMQ0052')
PE <ssid>.CHIN CL(MQCONN) ID(<WebSphereMQCHINUsrids>)
```

```
SETR RACL(MQCONN) REF
```

Note that an additional WebSphere MQ Refresh may be required for active Qmanagers. This is done from the

CONSOLE:

The example is for a Que Manager Named QMD1
 >QMD1 REFRESH SECURITY(*)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-224560

Group Title: ZWMQ0053

Rule ID: SV-7267r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0053

Rule Title: WebSphere MQ dead letter and alias dead letter queues are not properly defined.

Vulnerability Discussion: WebSphere MQ resources allow for the control of administrator functions, connections, commands, queues, processes, and namelists. Some resources provide the ability to disable or bypass security checking. Failure to properly protect WebSphere MQ resources may result in unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Systems Programmer

IAControls: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:

a) Create a report showing the WebSphere MQ channel definitions by submitting the JCL below. Add a job card and change the SSID value in the EXEC statement to your MQ SSID.

Note: This job must be run for each SSID.

```
//STEP1 EXEC PGM=CSQUTIL,PARM='SSID'
//STEPLIB DD DSN=CSQ700.SCSQAUTH,DISP=SHR
// DD DSN=CSQ700.SCSQANLE,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
COMMAND
//CSQUCMD DD *
DISPLAY SECURITY ALL
DISPLAY QUEUE(*) ALL
DISPLAY NAMELIST(*) ALL
DISPLAY PROCESS(*) ALL
DISPLAY CHANNEL(*) ALL
DISPLAY QMGR DEADQ
DISPLAY QMGR SSLKEYR
b)
```


1. Locate the start of the dead-letter queue information. Review the DEADQ parameter to obtain the name of the real dead-letter queue.
2. Find the QUEUE(dead-letter.queue.name) entry to locate the start of the real dead-letter queue definition. Review the GET and PUT parameters to determine their values, and ensure they conform to those specified in the Z/OS STIG.

The Z/OS STIG standard values are:

GET(ENABLED)
PUT(ENABLED)

NOTE: Dead-letter.queue.name is the value of the DEADQ parameter determined in Step 1.

2.1 If GET(ENABLED) and PUT(ENABLED) are specified, there is NO FINDING.

2.2 If GET(ENABLED) and PUT(ENABLED) are not specified, there is a FINDING.

3. From the top of the report, find the QUEUE(dead-letter.queue.name.PUT) entry to locate the start of the alias dead-letter queue definition.

Review the GET and PUT parameters to determine their values, and ensure they conform to those specified in the Z/OS STIG.

The Z/OS STIG standard values are:

GET(DISABLED)
PUT(ENABLED)

Note 1: Dead-letter.queue.name is the value of the DEADQ parameter determined in Step 1.

Note 2: The TARGQ parameter value for the alias queue will be the real dead-letter queue name.

Note 3: If an alias queue is not used in place of the dead-letter queue, then the RACF rules for the dead-letter queue must be coded to restrict unauthorized users and systems from reading the messages on the file.

3.1 If GET(DISABLED) and PUT(ENABLED) are specified, there is NO FINDING.

3.2 If GET(DISABLED) and PUT(ENABLED) are not, there is a FINDING.

4) Repeat these steps for each queue manager ssid.

c) If all of the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

Fix Text: The systems programmer responsible for supporting MQSeries/WebSphere MQ will ensure that the dead-letter queue and its alias are properly defined.

The following scenario describes how to securely define a dead-letter queue:

- (1) Define the real dead-letter queue with attributes PUT(ENABLED) and GET(ENABLED).
- (2) Give update authority for the dead-letter queue to CKTI (the MQSeries/WebSphere MQ-supplied CICS task initiator), channel initiators, and any automated application used for dead-letter queue maintenance.
- (3) Define an alias queue that resolves to the real dead-letter queue, but give the alias queue the attributes PUT(ENABLED) and GET(DISABLED).
- (4) To put a message on the dead-letter queue, an application uses the alias queue. The application does the following:
 - (a) Retrieve the name of the real dead-letter queue. To do this, it opens the queue manager object using MQOPEN, and then issues an MQINQ to get the dead-letter queue name.
 - (b) Build the name of the alias queue by appending the characters .PUT to this name, in this case, ssid.DEAD.QUEUE.PUT.
 - (c) Open the alias queue, ssid.DEAD.QUEUE.PUT.
 - (d) Put the message on the real dead-letter queue by issuing an MQPUT against the alias queue.
- (5) Give the userid associated with the application update authority to the alias, but no access to the real dead-letter queue.

NOTE: If an alias queue is not used in place of the dead-letter queue, then the ACP rules for the dead-letter queue will be coded to restrict unauthorized users and systems from reading the messages on the file.

Undeliverable messages can be routed to a dead-letter queue. Two levels of access should be established for these queues. The first level allows applications, as well as some MQSeries / WebSphere MQ objects, to put messages to this queue. The second level restricts the ability to get messages from this queue and protects sensitive data. This will be accomplished by defining an alias queue that resolves to the real dead-letter queue, but defines the alias queue with the attributes PUT(ENABLED) and GET(DISABLED). The ability to get messages from the dead-letter queue will be restricted to message channel agents (MCAs), CKTI (MQSeries/WebSphere MQ-supplied CICS task initiator), channel initiators utility, and any automated application used for dead-letter queue maintenance.

CCI: CCI-001762

Group ID (Vulid): V-224561

Group Title: ZWMQ0054

Rule ID: SV-7544r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0054

Rule Title: QUEUE Resources

Vulnerability Discussion: WebSphere MQ resources allow for the control of administrator functions, connections, commands, queues, processes, and namelists. Some resources provide the ability to disable or bypass security checking. Failure to properly protect WebSphere MQ resources may result in unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Use Administrator to analyze all profiles in the MQQUEUE and GMQUEUE resource classes.

1. From the Administrator main menu, type 3 on the command line (Security Server Reports) and press ENTER.
2. Type 4 on the command line (General Resource Reports) and press ENTER.
3. Tab down to CLASS: , type MQQUEUE or GMQUEUE, as appropriate, and press ENTER.

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

b) For all queue resources defined to the MQQUEUE or GMQUEUE resource classes, ensure the following items are in effect.

1. Resource profiles are defined with a UACC(NONE)
 - a. If all UACCs are equal to NONE, there is NO FINDING.
 - b. If any UACC is not equal to NONE, there is a FINDING.
2. For message queues (i.e., ssid.queueename), access authorization restricts access to users requiring the ability to get messages from and put messages to message queues. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.
 - a. If access authorization restricts access to users requiring the ability to get messages from and put messages to message queues, there is NO FINDING.
 - b. If access authorization allows access to users who do not require the ability to get messages from and put messages to message queues, there is a FINDING
3. For the system queues (i.e., ssid.SYSTEM.queueename), ALTER access authorization restricts access to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, systems programming personnel, and CICS regions running MQSeries/WebSphere MQ applications.

- a. If ALTER access authorization restricts access to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, systems programming personnel, and CICS regions running MQSeries/WebSphere MQ applications, there is NO FINDING.
 - b. If ALTER access authorization does not restrict access to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, systems programming personnel, and CICS regions running MQSeries/WebSphere MQ applications, there is a FINDING.
4. For the following system queues ensure that type LR in the CMD column next to them and ensure UPDATE access is restricted to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, CICS regions running WebSphere MQ applications, auditors, and users that require access to review message queues.

ssid.SYSTEM.COMMAND.INPUT
 ssid.SYSTEM.COMMAND.REPLY
 ssid.SYSTEM.CSQOREXX.*

- a. If the above System queues have update access limited to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, CICS regions running WebSphere MQ applications, auditors, and users that require access to review message queues, there is NO FINDING.
- b. If the above System queues DO NOT have update access limited to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, CICS regions running WebSphere MQ applications, auditors, and users that require access to review message queues, there is a FINDING.

5. For system queues (i.e., ssid.SYSTEM.CSQUTIL.*) ensure that UPDATE access is restricted to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, CICS regions running WebSphere MQ applications, and auditors.

- a. If the system queues (i.e., ssid.SYSTEM.CSQUTIL.*) have UPDATE access limited to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, CICS regions running WebSphere MQ applications, and auditors, there is NO FINDING.
- b. If the system queues (i.e., ssid.SYSTEM.CSQUTIL.*) DO NOT have UPDATE access limited to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, CICS regions running WebSphere MQ applications, and auditors, there is a FINDING.

6. Type LR in the CMD column of the real dead-letter queue (refer to STIG ID ZWMQ0053). Review the access list for the displayed profile.

- a. If access restricts access to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, CICS regions running MQSeries/WebSphere MQ applications, and any automated application used for dead-letter queue maintenance, there is NO FINDING2.
- b. If access authorization does not restrict access to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, CICS regions running MQSeries/WebSphere MQ applications, and any automated application used for dead-letter queue maintenance, there is a FINDING.

7. Type LR in the CMD column of the alias dead-letter queue (refer to STIG ID ZWMQ0053). Review the access list for the displayed profile.

- a. If access authorization restricts access to users requiring the ability to put messages to the dead-letter queue, there is NO FINDING.
- b. If access authorization does not restrict access to users requiring the ability to put messages to the dead-letter queue, there is a FINDING

8. Repeat steps a thru b for each profile in the GMQUEUE class.
- c) If all of the items in B were identified as NO FINDING, there is NO FINDING.
- d) If any of the items in B were identified as a FINDING, there is a FINDING.

Check Content:

Refer to the following report produced by the z/OS Data Collection:

- MQRPT(ssid)

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

Refer to the following reports produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(MQUEUE)

For all queue identified by the DISPLAY QUEUE(*) ALL command in the MQRPT(ssid). These queues will be prefixed by ssid to identify the resources to be protected. Ensure these queue resources are defined to the MQUEUE or GMQUEUE resource classes, if the following guidance is true, this is not a finding.

- 1) Resource profiles are defined with a UACC(NONE).
- 2) For message queues (i.e., ssid.queueename), access authorization restricts access to users requiring the ability to get messages from and put messages to message queues. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list. Decentralized MQ Administrators, non-DECC datacenter users; can have up to ALTER access to the user Message Queues.
- 3) For system queues (i.e., ssid.SYSTEM.queueename), access authorization restricts UPDATE and/or ALTER access to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, and CICS regions running WebSphere MQ applications.
- 4) For the following system queues ensure that UPDATE access is restricted to Auditors and Users that require access to review message queues.
 ssid.SYSTEM.COMMAND.INPUT
 ssid.SYSTEM.COMMAND.REPLY
 ssid.SYSTEM.CSQOREXX.*
- 5) For the real dead-letter queue (to determine queue name refer to ZWMQ0053), ALTER access authorization restricts access to WebSphere MQ STCs, WebSphere MQ administrators, CICS regions running WebSphere MQ applications, and any automated application used for dead-letter queue maintenance.
- 6) For the alias dead-letter queue (to determine queue name refer to ZWMQ0053), UPDATE access authorization restricts access to users requiring the ability to put messages to the dead-letter queue. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

Fix Text: For all queue resources defined to the MQUEUE or GMQUEUE resource classes, ensure the following items are in effect:

For all queue identified by the DISPLAY QUEUE(*) ALL command in the MQRPT(ssid). These queues will be prefixed by ssid to identify the resources to be protected. Ensure these queue resources are defined to the MQUEUE or GMQUEUE resource classes, if the following guidance is true, this is not a finding.

- 1) Resource profiles are defined with a UACC(NONE).
- 2) For message queues (i.e., ssid.queueename), access authorization restricts access to users requiring the ability to get messages from and put messages to message queues. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list. Decentralized MQ Administrators, non-DECC datacenter users; can have up to ALTER access to the user Message Queues.
- 3) For system queues (i.e., ssid.SYSTEM.queueename), access authorization restricts UPDATE and/or ALTER access to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, and CICS regions running WebSphere MQ applications.
- 4) For the following system queues ensure that UPDATE access is restricted to Auditors and Users that require access to review message queues.
 ssid.SYSTEM.COMMAND.INPUT
 ssid.SYSTEM.COMMAND.REPLY
 ssid.SYSTEM.CSQOREXX.*
 ssid.SYSTEM.CSQUTIL.*
- 5) For the real dead-letter queue (to determine queue name refer to ZWMQ0053), ALTER access authorization restricts access to WebSphere MQ STCs, WebSphere MQ administrators, CICS regions running WebSphere MQ applications, and any automated application used for dead-letter queue maintenance.
- 6) For the alias dead-letter queue (to determine queue name refer to ZWMQ0053), UPDATE access authorization restricts access to users requiring the ability to put messages to the dead-letter queue. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

Example:

```
RDEF MQQUEUE <ssid>.SYSTEM.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
DATA('REQUIRED FOR ZWMQ0054')
PE <ssid>.SYSTEM.** CL(MQQUEUE) ID(<RestrictedUsersAsSpecifiedAbove>)
```

```
RDEF MQQUEUE <ssid>.<qname>.* UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
DATA('REQUIRED FOR ZWMQ0054')
PE <ssid>.<qname> CL(MQQUEUE) ID(<AsSpecifiedAbove>)
```

```
RDEF MQQUEUE <ssid>.<RealDeadLetterQue>.* UACC(NONE) OWNER(ADMIN)
AUDIT(FAILURE(READ)) DATA('REQUIRED FOR ZWMQ0054')
PE <ssid>.<RealDeadLetterQue> CL(MQQUEUE) ID(<AsSpecifiedAbove>)
```

```
RDEF MQQUEUE <ssid>.<AliasDeadLetterQue>.* UACC(NONE) OWNER(ADMIN)
AUDIT(FAILURE(READ)) DATA('REQUIRED FOR ZWMQ0054')
PE <ssid>.<AliasDeadLetterQue> CL(MQQUEUE) ID(<AsSpecifiedAbove>)
```

```
SETR RACL(MQQUEUE) REF
```

CCI: CCI-000213

Group ID (Vulid): V-224562

Group Title: ZWMQ0055

Rule ID: SV-7546r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0055

Rule Title: WebSphere MQ Process resource profiles defined in the MQPROC Class are not protected in accordance with security requirements.

Vulnerability Discussion: WebSphere MQ Process resources allow for the control of processes. Failure to properly protect WebSphere MQ resources may result in unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Use Administrator to analyze all process name resource profiles in the MQPROC and GMQPROC resource classes.

1. From the Administrator main menu, type 3 on the command line (Security Server Reports) and press <ENTER>.
2. Type 4 on the command line (General Resource Reports) and press <ENTER>.
3. Tab down to CLASS: , type MQPROC, and press <ENTER>.
4. For all process name profiles displayed (i.e., ssid.processname) in the Profile Name column, review the corresponding UACC column.

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

b) For all process resources (i.e., ssid.processname) defined to the MQPROC or GMQPROC resource classes, ensure the following items are in effect:

NOTE 1: ssid is the queue manager name (a.k.a., subsystem identifier).

1. Resource profiles are defined with a UACC(NONE)
 - a. If all UACC s are equal to NONE, there is NO FINDING
 - b. If any UACC is not equal to NONE, there is a FINDING

Type LR in the CMD column of each profile. Review the access list for each displayed profile.

2. Restrict access to users requiring the ability to make process inquiries.

Note: Identifying users authorized to make process inquiries is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

- a. If access authorization restricts access to users requiring the ability to make process inquiries, there is NO FINDING.
- b. If access authorization allows access to users who do not require the ability to make process inquiries, there is a FINDING

Repeat steps (a) thru (b) for each profile in the GMQPROC class.

- c) If all of the items in B were identified as NO FINDING, there is NO FINDING.
- d) If any of the items in B were identified as a FINDING, there is a FINDING.

Fix Text: Process security validates userids authorized to issue MQSeries / WebSphere MQ inquiries on process definitions. A process definition object defines an application that is started in response to a trigger event on a queue manager. Process security will be active, and all profiles ssid.processname will be defined to the MQPROC class. Restrict read access to those userids requiring access to make process inquiries.

For all process resources (i.e., ssid.processname) defined to the MQPROC or GMQPROC resource classes, ensure the following items are in effect:

NOTE 1: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) Resource profiles are defined with a UACC(NONE).
- 2) Access authorization restricts access to users requiring the ability to make process inquiries. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

A set of sample commands are provided below to implement the minimum profiles necessary for proper security.

/* THE FOLLOWING PROFILE FORCES GRANULAR PROFILES DEFINITIONS */

RDEF MQPROC ** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQPROC DENY-BY-DEFAULT PROFILE')

RDEF MQPROC <ssid>.* UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('REQUIRED FOR ZWMQ0055')

PE <ssid>.* CL(MQPROC) ID(<ApplicableUsers>)

SETR RACL(MQPROC) REF

Note that an additional WebSphere MQ Refresh may be required for active Qmanagers. This is done from the CONSOLE:

The example is for a Que Manager Named QMD1
>QMD1 REFRESH SECURITY(*)

The following is a sample of the commands required to allow a group (GRP1) to inquire on processes beginning with the letter V on queue manager (QM1):

RDEFINE MQPROC QM1.V* UACC(NONE) AUDIT(ALL(READ))
PERMIT QM1.V* CLASS(MQPROC) ID(GRP1) ACCESS(READ)

CCI: CCI-000213

Group ID (Vulid): V-224563

Group Title: ZWMQ0056

Rule ID: SV-7548r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0056

Rule Title: WebSphere MQ Namelist resource profiles defined in the MQNLIST Class are not protected in accordance with security requirements.

Vulnerability Discussion: WebSphere MQ resources allow for the control of administrator functions, connections, commands, queues, processes, and namelists. Some resources provide the ability to disable or bypass security checking. Failure to properly protect WebSphere MQ resources may result in unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Use Administrator to analyze all namelist resource profiles in the MQNLIST and GMQNLIST resource classes.

1. From the Administrator main menu, type 3 on the command line (Security Server Reports) and press <ENTER>.
2. Type 4 on the command line (General Resource Reports) and press <ENTER>.
3. Tab down to CLASS: , type MQNLIST, and press <ENTER>.
4. For all profiles displayed in the Profile Name column, review the corresponding UACC column.

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

b) For all namelist resources (i.e., ssid.namelist) defined to the MQNLIST or GMQNLIST resource classes, ensure the following items are in effect:

NOTE 1: ssid is the queue manager name (a.k.a., subsystem identifier).

1. Resource profiles are defined with a UACC(NONE)
 - a. If all UACC s are equal to NONE, there is NO FINDING
 - b. If any UACC is not equal to NONE, there is a FINDING

Type LR in the CMD column of each profile. Review the access list for each displayed profile.

2. Restrict access to users requiring the ability to make namelist inquiries.

Note: Identifying users authorized to make namelist inquiries is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

- a. If access authorization restricts access to users requiring the ability to make namelist inquiries, there is NO FINDING2.
- b. If access authorization allows access to users who do not require the ability to make namelist inquiries, there is a FINDING.

Repeat steps (a) thru (b) for the GMQNLIST class.

c) If all of the items in B were identified as NO FINDING, there is NO FINDING.

d) If any of the items in B were identified as a FINDING, there is a FINDING.

Fix Text: A namelist is a MQSeries / WebSphere MQ object that contains a list of queue names. Namelist security validates userids authorized to inquire on namelists. Namelist security will be active, and all profiles ssid.namelist will be defined to the MQNLIST or GMQNLIST class with UACC(NONE) specified. Restrict read access to those userids requiring access to make namelist inquiries.

For all namelist resources (i.e., ssid.namelist) defined to the MQNLIST or GMQNLIST resource classes, ensure the following items are in effect:

NOTE 1: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) Resource profiles are defined with a UACC(NONE).
- 2) Access authorization restricts access to users requiring the ability to make namelist inquiries. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

A set of sample commands are provided below to implement the minimum profiles necessary for proper security.

/* THE FOLLOWING PROFILE FORCES GRANULAR PROFILES DEFINITIONS */

RDEF MQNLIST ** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQCONN DENY-BY-DEFAULT PROFILE')

RDEF MQNLIST <ssid>.* UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('REQUIRED FOR ZWMQ0056')

PE <ssid>.* CL(MQNLIST) ID(<applicable>)

SETR RACL(MQNLIST) REF

Note that an additional WebSphere MQ Refresh may be required for active Qmanagers. This is done from the CONSOLE:

The example is for a Que Manager Named QMD1
>QMD1 REFRESH SECURITY(*)

CCI: CCI-000213

Group ID (Vulid): V-224564

Group Title: ZWMQ0057

Rule ID: SV-7550r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0057

Rule Title: WebSphere MQ Alternate User resources defined to MQADMIN resource class are not protected in accordance with security requirements.

Vulnerability Discussion: WebSphere MQ resources allow for the control of administrator functions, connections, commands, queues, processes, and namelists. Some resources provide the ability to disable or bypass security checking. Failure to properly protect WebSphere MQ resources may result in unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and

customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Use Administrator to analyze all alternative resource profiles in the MQADMIN resource classes.

1. From the Administrator main menu, type 3 on the command line (Security Server Reports) and press <ENTER>.

2. Type 4 on the command line (General Resource Reports) and press <ENTER>.

3. Tab down to CLASS: , type MQADMIN and press <ENTER>

4. For all alternate user resources (i.e. ssid.ALTERNATE.USER.alternateuserid) displayed in the Profile Name column, review the corresponding UACC column

5. Type LR in the CMD column of each alternate user resource (i.e. ssid.ALTERNATE.USER.alternateuserid). Review the access list for each displayed profile.

b) For all alternate user resources (i.e., ssid.ALTERNATE.USER.alternateuserid) defined to the MQADMIN resource class, ensure the following items are in effect:

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

1. Resource profiles are defined with a UACC(NONE).

2. Access authorization restricts access to users requiring the ability to use the alternate userid. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

c) If both of the items in (b) are true, there is NO FINDING.

d) If either item in (b) is untrue, this is a FINDING.

Fix Text: Alternate userid security allows access to be requested under another userid. Alternate userid security will be active, and all profiles ssid.ALTERNATE.USER.alternateuserid will be defined to the MQADMIN class with UACC(NONE) specified. Restrict update access to those userids requiring access to alternate userids.

For all alternate user resources (i.e., ssid.ALTERNATE.USER.alternateuserid) defined to the MQADMIN resource class, ensure the following items are in effect:

NOTE 1: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) Resource profiles are defined with a UACC(NONE).
- 2) Access authorization restricts access to users requiring the ability to use the alternate userid. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

A set of sample commands are provided below to implement the minimum profiles necessary for proper security.

/* THE FOLLOWING PROFILE FORCES GRANULAR PROFILES DEFINITIONS */

RDEF MQADMIN ** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQADMIN DENY-BY-DEFAULT PROFILE')

RDEF MQADMIN <ssid>.ALTERNATE.USER.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQADMIN DENY-BY-DEFAULT for ALT USER PROFILE')

The following is a sample of the commands required to allow payroll server (PAYSRV1) to specify alternate userids starting with the characters PS on queue manager (QM1):

RDEFINE MQADMIN QMD1.ALTERNATE.USER.PS* UACC(NONE) AUDIT(ALL)

PERMIT QMD1.ALTERNATE.USER.PS* CLASS(MQADMIN) ID(PAYSRV1) ACCESS(UPDATE)

SETR RACL(MQADMIN) REF

Note that an additional WebSphere MQ Refresh may be required for active Qmanagers. This is done from the CONSOLE:

The example is for a Que Manager Named QMD1
>QMD1 REFRESH SECURITY(*)

CCI: CCI-000213

Group ID (Vulid): V-224565

Group Title: ZWMQ0058

Rule ID: SV-7552r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0058

Rule Title: CONTEXT Resources

Vulnerability Discussion: Context security validates whether a userid has authority to pass or set identity and/or origin data for a message. Context security will be active to avoid security exposure.

This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Use Administrator to analyze all context resource profiles in the MQADMIN resource class.

1. From the Administrator main menu, select 3 (Security Server Reports) and press <ENTER>.
2. Type 4 on the command line (General Resource Reports) and press <ENTER>.
3. Tab down to CLASS: , type MQADMIN and press <ENTER>.
4. For all context resources (i.e., ssid.CONTEXT) displayed in the Profile Name column, review the corresponding UACC column.
5. Type LR in the CMD column of each context resource profile (i.e., ssid.CONTEXT). Review the access list for each displayed profile.

b) For all context resources defined to the MQADMIN resource classes, ensure the following items are in effect.

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

Access authorization restricts access to users requiring the ability to pass or set identity and/or origin data for a message. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

1. If all UACC s are equal to NONE, there is NO FINDING.
2. If any UACC is not equal to NONE, there is a FINDING.
3. If access authorization restricts access to users authorized to use the alternate userid, there is NO FINDING
4. If access authorization allows users who are not authorized to use the alternate userid, there is a FINDING

Fix Text: Context security validates whether a userid has authority to pass or set identity and/or origin data for a message. Context security will be active, and all profiles ssid.CONTEXT will be defined to the MQADMIN class with UACC(NONE) specified, where ssid is the queue manager name.

Read access is required when the PASS option is specified for an MQOPEN or MQPUT1. Update or control access is required when the SET or OUTPUT option is specified.

For all context resources (i.e., ssid.CONTEXT) defined to the MQADMIN resource class, ensure the following items are in effect:

NOTE 1: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) Resource profiles are defined with a UACC(NONE).
- 2) Access authorization restricts access to users requiring the ability to pass or set identity and/or origin data for a message. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.

A set of sample commands are provided below to implement the minimum profiles necessary for proper security.

```
/* THE FOLLOWING PROFILE FORCES GRANULAR PROFILES DEFINITIONS */
```

```
RDEF MQADMIN ** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQADMIN DENY-  
BY-DEFAULT PROFILE')
```

```
RDEF MQADMIN <ssid>.CONTEXT UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))  
DATA('MQADMIN PROFILE REQUIRED FOR CONTEXT SECURITY')
```

The following is a sample of the commands required to allow a systems programming group (SYS1) to offload and reload messages for queue manager (QMD1):

```
PERMIT QMD1.CONTEXT CLASS(MQADMIN) ID(SYS1) ACCESS(CONTROL)
```

The following refresh is required for RACListed classes:

```
SETR RACL(MQADMIN) REF
```

Note that an additional WebSphere MQ Refresh may be required for active Qmanagers. This is done from the CONSOLE:

The example is for a Que Manager Named QMD1
>QMD1 REFRESH SECURITY(*)

CCI: CCI-000213

Group ID (Vulid): V-224566

Group Title: ZWMQ0059

Rule ID: SV-7554r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0059

Rule Title: WebSphere MQ command resources defined to MQCMD5 resource class are not protected in accordance with security requirements.

Vulnerability Discussion: WebSphere MQ resources allow for the control of commands. Failure to properly protect WebSphere MQ Command resources may result in unauthorized access. This exposure could compromise the availability, integrity, and confidentiality of system services, applications, and customer data.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Use Administrator to analyze all command resource profiles (i.e., ssid.command) in the MQCMD5 resource class.

1. From the Administrator main menu, select 3 (Security Server Reports) and press <ENTER>.
2. Type 4 on the command line (General Resource Reports) and press <ENTER>.
3. Tab down to CLASS: , type MQCMD5 and press <ENTER>.

4. For all command resource profiles (i.e., ssid.command) displayed in the Profile Name column, review the corresponding UACC column.
5. Type LR in the CMD column of each command resource profile (i.e., ssid.command). Review the access list and audit attributes for each displayed profile.

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

b) For all command resources (i.e., ssid.command) defined to the MQCMDS resource class, ensure the following items are in effect:

1. Review the universal access for each displayed profile.

- a. If all UACC s are equal to NONE, there is NO FINDING.
- b. If any UACC is not equal to NONE, there is a FINDING.

2. Review the audit attributes for each displayed profile.

- a. If all command access is logged as designated in the table entitled Command Security Controls in in the U_zOS_STIG_Addendum, there is NO FINDING
- b. If all command access is not logged as designated in the table entitled Command Security Controls in in the U_zOS_STIG_Addendum this is a FINDING

3. Review the access list for each displayed profile.

- a. If access authorization is restricted to appropriate personnel as designated in the table entitled Websphere MQ COMMAND SECURITY CONTROLS Table in the z/OS STIG Addendum there is NO FINDING.
- b. If access authorization is not restricted to appropriate personnel as designated Websphere MQ COMMAND SECURITY CONTROLS Table in the z/OS STIG Addendum, there is a FINDING.

- c) If all of the items in (b) were identified as NO FINDING, there is NO FINDING.

- d) If any of the items in (b) were identified as a FINDING, there is a FINDING.

Fix Text: Command security validates userids authorized to issue MQSeries / WebSphere MQ commands. Command security will be active

For all command resources (i.e., ssid.command) defined to the MQCMDS resource class, ensure the following items are in effect:

NOTE 1: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) Resource profiles are defined with a UACC(NONE).
- 2) Access authorization restricts access to the appropriate personnel as designated in the table entitled "Websphere MQ Command Security Controls " in the zOS STIG Addendum.
- 3) All command access is logged as designated in the table entitled "Websphere MQ Command Security Controls" in the zOS STIG Addendum.

A set of sample commands are provided below to implement the minimum profiles necessary for proper security.

/* THE FOLLOWING PROFILE FORCES GRANULAR PROFILES DEFINITIONS */

RDEF MQCMDS ** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQCMDS DENY-BY-DEFAULT PROFILE')

RDEF MQCMDSN <ssid>.<CmdName>.* UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('MQCMDS Required See ZWMQ0059')

PE <ssid>.<CmdName>.* CL(MQCMDS) ID(<authorizeduser>) ACC(C)

SETR RACL(MQCMDS) REF

Note that an additional WebSphere MQ Refresh may be required for active Qmanagers. This is done from the CONSOLE:

The example is for a Que Manager Named QMD1
>QMD1 REFRESH SECURITY(*)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-224567

Group Title: ZWMQ0060

Rule ID: SV-7556r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZWMQ0060

Rule Title: RESLEVEL Resources

Vulnerability Discussion: RESLEVEL security profiles control the number of userids checked for API-resource security.

RESELEVEL is a powerful option that can cause the bypassing of all security checks.

RESELEVEL security will not be implemented.

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) Refer to the following reports produced by the Data Set and Resource Data Collection:

- SENSITIVE.RPT(MQADMIN)

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZWMQ0060)

b) Ensure the following items are in effect:

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) A RESLEVEL resource (i.e., ssid.RESLEVEL) is defined for each queue manager to the MQADMIN resource class with a UACC(NONE).
 - 2) Access authorization to these RESLEVEL resources restricts all access. No users or groups must be specified in the access list.
- c) If both of the items in (b) are true, there is NO FINDING.
- d) If either item in (b) is untrue, this is a FINDING.

Fix Text: RESLEVEL security profiles control the number of userids checked for API-resource security. RESLEVEL security will not be implemented due to the following exposures and limitations:

- (1) RESLEVEL is a powerful option that can cause the bypassing of all security checks.
- (2) Security audit records are not created when the RESLEVEL profile is utilized.
- (3) If the WARNING option is specified on a RESLEVEL profile, no warning messages are produced.

To protect against any profile in the MQADMIN class, such as ssid.**, resolving to a RESLEVEL profile, a ssid.RESLEVEL profile will be defined for each queue manager with UACC(NONE) specified and no users or groups specified in the access list.

Ensure the following items are in effect:

NOTE: ssid is the queue manager name (a.k.a., subsystem identifier).

- 1) A RESLEVEL resource (i.e., ssid.RESLEVEL) is defined for each queue manager to the MQADMIN resource class with a UACC(NONE).
- 2) Access authorization to these RESLEVEL resources restricts all access. No users or groups must be specified in the access list.

A set of sample commands are provided below to implement the profile necessary for proper security.

```
RDEF MQADMIN <ssid>.RESLEVEL UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
DATA('MQADMIN PROFILE REQUIRED BY ZWMQ0060')
```

```
SETR RACL(MQADMIN) REF
```

Note that an additional WebSphere MQ Refresh may be required for active Qmanagers. This is done from the CONSOLE:

```
The example is for a Que Manager Named QMD1
>QMD1 REFRESH SECURITY(*)
```

CCI: CCI-000213

CCI: CCI-001762

UNCLASSIFIED