VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

z/OS CA MIM for TSS STIG

Version: 6

Release: 3

20 Jan 2015

_____

Group ID (Vulid): V-18014
Group Title: ZB000040
Rule ID: SV-46150r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZMIM0040
Rule Title: CA MIM Resource Sharing external security options must be specified properly.

Vulnerability Discussion: CA MIM Resource Sharing offers external security interfaces that are controlled by parameters specified in the MIMINIT member in the MIMPARMS DD statement of the started task procedures. These interfaces provide security controls for CA MIM. Without proper controls to ensure that security is active, the integrity of the CA MIM Resource Sharing System and the confidentiality of data stored on the system may be compromised.

IAControls: ECCD-1, ECCD-2

Check Content:
Refer to the contents of MIMINIT member of the data set(s) specified in the MIMPARMS DD statement of the started task procedures.

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

-      PDI(ZMIM0040)

Ensure the following CA MIM Resource Sharing parameter(s) is (are) specified in the MIMINIT member of the data set(s) specified in the MIMPARMS DD statement of the started task procedures. If the following guidance is true, this is not a finding.

Parameter   Value
SAFCMDAUTH   ON

Fix Text: The systems programmer/IAO will ensure that the CA MIM Resource Sharing parameter(s) is (are) specified. CA MIM Resource Sharing security interfaces are controlled by parameters coded in the MIMINIT member of the data set(s) specified in the MIMPARMS DD statement of the started task procedures.

Parameter   Value
SAFCMDAUTH   ON

CCI: CCI-000035

_____

Group ID (Vulid): V-16932

Group Title: ZB000000
Rule ID: SV-46160r1_rule
Severity: CAT II
 Rule Version (STIG-ID): ZMIMT000
Rule Title: CA MIM Resource Sharing installation data sets will be properly protected.

Vulnerability Discussion: CA MIM Resource Sharing installation data sets have the ability to use privileged functions and/or have access to sensitive data. Failure to properly restrict access to these data sets could result in violating the integrity of the base product which could result in compromising the operating system or sensitive data.

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

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

-       SENSITVE.RPT(MIMRPT)

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

-       PDI(ZMIM0000)

Verify that the accesses to the CA MIM Resource Sharing installation data sets are properly restricted. If the following guidance is true, this is not a finding.

___   The TSS data set access authorizations restricts READ access to all authorized users.

___   The TSS data set access authorizations restricts WRITE and/or greater access to systems programming personnel.

___   The TSS data set access authorizations specify that all (i.e., failures and successes) WRITE and/or greater access are logged.

Fix Text: The IAO will ensure that WRITE and/or greater access to CA MIM Resource Sharing installation data sets is limited to System Programmers only, and all WRITE and/or greater access is logged. READ access can be given to all authorized users. All failures and successful WRITE and/or greater accesses are logged.

The installing Systems Programmer will identify and document the product data

sets and categorize them according to who will have WRITE and/or greater access and if required that all WRITE and/or greater access is logged. He will identify if any additional groups have WRITE and/or greater 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.

(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.)

Data sets to be protected will be:
SYS2.MIMGR.
SYS3.MIMGR. (data sets that are not altered by product STCs, can be more specific)

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

TSS PERMIT(<syspaudt>) DSN(SYS2.MIMGR.) ACCESS(R)
TSS PERMIT(<syspaudt>) DSN(SYS2.MIMGR.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<tstcaudt>) DSN(SYS2.MIMGR.) ACCESS(R)
TSS PERMIT(<tstcaudt>) DSN(SYS2.MIMGR.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<audtaudt>) DSN(SYS2.MIMGR.) ACCESS(R)
TSS PERMIT(authorized users) DSN(SYS2.MIMGR.) ACCESS(R)
TSS PERMIT(CA MIM STCs) DSN(SYS2.MIMGR.) ACCESS(R)
TSS PERMIT(<syspaudt>) DSN(SYS3.MIMGR.) ACCESS(R)
TSS PERMIT(<syspaudt>) DSN(SYS3.MIMGR.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<tstcaudt>) DSN(SYS3.MIMGR.) ACCESS(R)
TSS PERMIT(<tstcaudt>) DSN(SYS3.MIMGR.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<audtaudt>) DSN(SYS3.MIMGR.) ACCESS(R)
TSS PERMIT(authorized users) DSN(SYS3.MIMGR.) ACCESS(R)
TSS PERMIT(CA MIM STCs) DSN(SYS3.MIMGR.) ACCESS(R)

CCI: CCI-000213

CCI: CCI-002234

_____

 Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-46167r1_rule
Severity: CAT II
 Rule Version (STIG-ID): ZMIMT001
Rule Title: CA MIM Resource Sharing STC data sets will be properly protected.

Vulnerability Discussion: CA MIM Resource Sharing STC data sets have the ability to use privileged functions and/or have access to sensitive data. Failure to properly restrict access to these data sets could result in violating the integrity of the base product which could result in compromising the operating system or sensitive data.

IAControls: DCSL-1, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

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

-    SENSITVE.RPT(MIMSTC)

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

-    PDI(ZMIM0001)

Verify that the accesses to the CA MIM Resource Sharing STC data sets are properly restricted. If the following guidance is true, this is not a finding.

___   The TSS data set access authorizations restrict READ access to auditors and authorized users.

___   The TSS data set access authorizations restrict WRITE and/or greater access to systems programming personnel.

___   The TSS data set access authorizations restrict WRITE and/or greater access to the CA MIM Resource Sharing's STC(s) and/or batch user(s).

Fix Text: The IAO will ensure that WRITE and/or greater access to CA MIM Resource Sharing STC data sets is limited to System Programmers and/or CA MIM Resource Sharing's STC(s) and/or batch user(s) only. Read access can be given to auditors and authorized users.

The installing Systems Programmer will identify and document the product data sets and categorize them according to who will have WRITE and/or greater access and if required that all WRITE and/or greater access is logged. He will identify if any additional groups have WRITE and/or greater 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.

(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.)

Data sets to be protected will be:
SYS3.MIMGR. (Data sets that are altered by the product's STCs, this can be more specific.)

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

TSS PERMIT(<syspaudt>) DSN(SYS3.MIMGR) ACCESS(ALL)
TSS PERMIT(<tstcaudt>) DSN(SYS3.MIMGR) ACCESS(ALL)
TSS PERMIT(CA MIM STCs) DSN(SYS3.MIMGR) ACCESS(ALL)
TSS PERMIT(<audtaudt>) DSN(SYS3.MIMGR) ACCESS(R)
TSS PERMIT(authorize user) DSN(SYS3.MIMGR) ACCESS(R)

CCI: CCI-001499

_____

Group ID (Vulid): V-17947
Group Title: ZB000020
Rule ID: SV-46209r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZMIMT020
Rule Title: CA MIM Resource Sharing resources will be properly defined and protected.

Vulnerability Discussion: CA MIM Resource Sharing can run with sensitive system privileges, and potentially can circumvent system controls. Failure to properly control access to product resources could result in the compromise of the operating system environment, and compromise the confidentiality of customer data. Many utilities assign resource controls that can be granted to system programmers only in greater than read authority. Resources are also granted to certain non systems personnel with read only authority.

IAControls: ECCD-1, ECCD-2

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

-    SENSITVE.RPT(ZMIM0020)
-    TSSCMDS.RPT(#RDT)

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

-    PDI(ZMIM0020)

Verify that the accesses to resources and/or generic equivalent are properly restricted according to the requirements specified in CA MIM Resource Sharing Resources table in the z/OS STIG Addendum. If the following guidance is true, this is not a finding.

___   The TSS resources are owned or DEFPROT is specified for the resource class.

___   The TSS resource access authorizations restrict access to the appropriate personnel.

Fix Text: The IAO will work with the systems programmer to verify that the following are properly specified in the ACP.

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

Use CA MIM Resource Sharing Resources table in the zOS STIG Addendum. This table list the resources, access requirements, and logging requirement for CA MIM Resource Sharing. Ensure the guidelines for the resources and/or generic equivalent specified in the z/OS STIG Addendum are followed.

Note: SAFPREFIX identifies the prefix for all resources. The default value for this keyword parameter is MIMGR. It is coded in the MIMINIT member of the data set specified in the MIMPARMS DD statement of the started task procedures.

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

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

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

TSS ADD(dept-acid) OPERCMDS(prefix)
TSS PERMIT(syspaudt) OPERCMDS(prefix.ACTIVATE) ACCESS(UPDATE)

CCI: CCI-000035

CCI: CCI-002234

_____

Group ID (Vulid): V-17452

Group Title: ZB000030
Rule ID: SV-46212r1_rule
Severity: CAT II
 Rule Version (STIG-ID): ZMIMT030
Rule Title: CA MIM Resource Sharing Started Task name will be properly
identified and/or defined to the system ACP.

Vulnerability Discussion: CA MIM Resource Sharing 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.

IAControls: ECCD-1, ECCD-2

Check Content:
Refer to the following report produced by the TSS Data Collection:

-       TSSCMDS.RPT(@ACIDS)

Verify that the ACID(s) for the CA MIM Resource Sharing started task(s) is (are)
properly defined. If the following attributes are defined, this is not a
finding.

FACILITY(STC, BATCH)
PASSWORD(xxxxxxxx,0)
SOURCE(INTRDR)
NOSUSPEND

Fix Text: The IAO working with the systems programmer will ensure the CA MIM
Resource Sharing Started Task(s) is properly identified and/or defined to the
System ACP.

If the product requires a Started Task, verify that it is properly defined to
the System ACP with the proper attributes.

Most installation manuals will indicate how the Started Task is identified and
any additional attributes that must be specified.

The following commands are provided as a sample for defining Started Task(s):

TSS CREATE(MIMGR) TYPE(USER) -
     NAME('STC, CA MIM') DEPT(xxxx) -
     FAC(STC,BATCH) PASS(xxxxxxxx,0) -
     SOURCE(INTRDR) NOSUSPEND

CCI: CCI-000764

_____

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-46214r1_rule
Severity: CAT II
 Rule Version (STIG-ID): ZMIMT032
Rule Title: CA MIM Resource Sharing Started task will be properly defined to the
Started Task Table for Top Secret.

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.

IAControls: ECCD-1, ECCD-2

Check Content:
Refer to the following report produced by the TSS Data Collection:

-      TSSCMDS.RPT(#STC)

Automated Analysis
Refer to the following report produced by the TSS Data Collection:

-      PDI(ZMIM0032)

If the CA MIM Resource Sharing started task(s) is (are) defined in the TSS STC
record, this is not a finding.

Fix Text: The IAO working with the systems programmer will ensure the CA MIM
Resource Sharing Started Task(s) is properly identified and/or defined to the
System ACP.

A unique ACID must be assigned for the CA MIM Resource Sharing started task(s)
thru a corresponding STC table entry.

The following commands are provided as a sample for defining Started Task(s):

TSS ADD(STC) PROCNAME(MIMGR) ACID(MIMGR)

CCI: CCI-000764

_____