

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

z/OS CA MIM for RACF STIG

Version: 6

Release: 5

30 June 2023

XSL Release 5/15/2012 Sort by: STIGID
Description:

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.

Responsibility: Information Assurance Officer
IAControls: ECCD-1, ECCD-2

Check Content:

- a) Find the name of the dataset specified in the MIMPARMS DD statement in the CAMIM started task procedure.
- b) Check member MIMINIT in the dataset specified in a) above for the setting of the parameter SAFCFMDAUTH .
- c). If the setting of this parameter is "ON", there is NO FINDING.
- d) If the setting of this parameter is not "ON", there is a FINDING.

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-46159r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZMIMR000
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.

Responsibility: Information Assurance Officer
IACControls: DCSL-1, ECAR-1, ECAR-2, ECCD-1, ECCD-2

Check Content:

a) Consult with your systems programmer to identify the names of the CA MIM

resource sharing product installation datasets (they may likely be called or

begin with

SYS2.MIMGR, SYS3.MIMGR).

b) Ensure the following data set controls are in effect for the CA-MIM resource

sharing

installation data sets:

- READ access to the CA MIM resource sharing installation data sets is restricted to all authorized users.

- UPDATE or higher access to the CA MIM resource sharing installation data sets

is restricted to systems programming personnel.

- UACC (None) and NOWARNING are specified for the CA MIM resource sharing

installation data sets.

- The RACF data set rules for the CA MIM resource sharing installation data

sets

specify that all accesses of UPDATE or higher (i.e., failures and successes)

are

logged.

c) Verify as follows:

1. From the Administrator main menu, select 3.3 (Dataset Profile Reports) and

press ENTER.

2. Tab down to the Data Set rows and type LV next to the dataset profile for

the

first CA MIM data set.

3. Check that UACC = None and Warning = No on the dataset profile General

Information Screen.

4. Review the Standard Access List and Conditional Access List on the dataset

profile General Information Screen. and verify that access is restricted as

specified in b. above.

5. Verify the 'Audit Successes' column on the dataset profile General Information

screen . Underneath it should be found 'Successes Write' which means that all

successful UPDATE access is logged as specified in b.above.

6. Verify the 'Audit Failures' column on the dataset profile General Information

screen . Underneath it should be found 'Failures Write' which means that all

failed UPDATE access is logged as specified in b. above.

7. Repeat steps 1-6 above for any other CA MIM dataset profiles.

d) If UPDATE access or higher to the CA MIM installation data sets are

restricted to

systems programming personnel, there is NO FINDING.

e) If UPDATE access or higher to the CA MIM installation data sets are

not

restricted to systems programming personnel there is a FINDING.

f) If UACC = None and Warning = No there is NO FINDING.

g) If UACC is not None or Warning is not No, there is a FINDING.

h) If all accesses of UPDATE or higher are logged there is NO FINDING.

i) If all accesses of UPDATE or higher are not logged, there is a FINDING.

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:

```
ad 'SYS2.MIMGR.**' uacc(none) owner(sys2) -
    audit(success(update) failures(read)) -
    data('CA MIM Resource Sharing Install DS')
pe 'SYS2.MIMGR.**' id(<syspaudt> <tstcaudt>) acc(a)
pe 'SYS2.MIMGR.**' id(<audtaudt> authorized users) acc(r)
pe 'SYS2.MIMGR.**' id(CA MIM STCs)
```

```
ad 'SYS3.MIMGR.**' uacc(none) owner(sys3) -
    audit(success(update) failures(read)) -
    data('CA MIM Resource Sharing Install DS')
pe 'SYS3.MIMGR.**' id(<syspaudt> <tstcaudt>) acc(a)
pe 'SYS3.MIMGR.**' id(<audtaudt> authorized users) acc(r)
pe 'SYS3.MIMGR.**' id(CA MIM STCs)
```

setr generic(dataset) refresh

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067
 Group Title: ZB000001
 Rule ID: SV-46166r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZMIMR001
 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.

Responsibility: Information Assurance Officer
IACcontrols: DCSL-1, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:

a) Consult with your systems programmer to identify the names of the CA MIM

resource

sharing product STC datasets (they may likely be called or begin with SYS3.MIGR).

b) Ensure the following data set controls are in effect for the CA MIM resource

sharing

STC data sets:

- READ access to the CA MIM resource sharing product STC data sets can be given

to auditors and authorized users.

- UPDATE or higher access to the CA MIM resource sharing product STC data sets

is restricted to systems programming personnel and/or CA MIM s STCs and/or batch users.

- UACC (None) and NOWARNING are specified for the CA MIM resource sharing

products STC data sets.

- The RACF data set rules for the CA MIM resource sharing STC data sets specify

that all accesses of UPDATE or higher (i.e., failures and successes) will be

logged if

required by the IAO..

c) Verify as follows:

1 From the Administrator main menu, select 3.3 (Dataset Profile Reports) and

press ENTER.

2. Tab down to Data Set row, type LV next to the dataset profile for the first CA MIM resource sharing STC data sets.

3. Check that UACC = None and Warning = No on the dataset profile

General

Information Screen.

4. Review the Standard Access List and Conditional Access List areas on the

dataset profile General Information Screen and verify that access is restricted

as

specified in b.above.

5. If required by the IAO Verify the 'Audit Successes' and 'Audit Failures'

column on the dataset profile General Information screen. .They should match

the access required (probably 'Successes Write' and 'Failures Write' respectively).

6. Repeat steps 1-5 above for any other CA MIM resource sharing STC dataset profiles.

d) If UPDATE and ALLOCATE (e.g. ALTER) access to the CA MIM resource sharing STC data sets are specified as in b. above, there is NO FINDING.

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:

```
ad 'SYS3.MIMGR.**' uacc(none) owner(sys3) -
    audit(failures(read)) -
    data('Vendor DS Profile: CA MIM Resource Sharing')
pe 'SYS3.MIMGR.**' id(<syspautd> <tstcaudt> CA MIM STCs) acc(a)
pe 'SYS3.MIMGR.**' id(<audtaudt> authorized users) acc(r)
```

```
setr generic(dataset) refresh
```

CCI: CCI-001499

Group ID (Vulid): V-17947
 Group Title: ZB000020
 Rule ID: SV-46208r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZMIMR020
 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.

Responsibility: Information Assurance Officer
 IACControls: ECCD-1, ECCD-2

Check Content:

- a) From the Administrator main menu, select 3;4 (Security Server Reports, General Resource Profiles) and press ENTER.
- b) Tab down to Profile . The default CA MIM profile prefix is MIMGR and if the default has been used enter MIMGR.* as the generic resource profile name and hit enter to bring up the General Resource Profile Summary screen listing all the CA MIM resources.
 To determine if the default profile prefix has been used
 - find the name of the data set specified on the MIMPARMS DD statement of the started task procedure.
 - find member MIMINIT in the dataset
 - the value specified in MIMINIT is the prefix for CA MIM resource profiles.
- c) Check the profiles that are displayed on the General Resource Profile Summary screen. For any profiles on the display that are found in the CA MIM RESOURCE SHARING RESOURCES table found in the z/OS STIG addendum:
 1. Verify that they are defined with a UACC=NONE.
 2. Type LR in the CMD column of each resource name and check that:
 - Warning is set to NO
 - The list of users and conditional access users only include

users that belong to the groups specified in the CA MIM RESOURCE SHARING RESOURCES table.

** (To check if a user belongs to one of the groups in the CA MIM RESOURCES SHARING RESOURCES table:
- Select Option 3;2 from the Administrator Main Menu (Security Server Reports, Group Profiles)
- On the Group Reports Menu, enter 1 at the Command line (for Group Profile Summary)
- Then tab down to Group and enter the Group Name from the resources table and hit enter.
- On the next panel enter LV next to the group name and hit enter.
- The General Information Screen that comes up will have the list of Connected Users

d) If
- WARNING is not set to NO or
- UACC is not NONE or
- any users are granted access who are not in the CA MIM Resource Sharing Resources table there is a FINDING.

e) If none of the conditions in d) above are true, then there is NO FINDING..

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 RACF resources as designated in the above table are defined with a default

access of NONE.

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

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

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

```
RDEFINE OPERCMDS prefix.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
RDEFINE OPERCMDES prefix.ACTIVATE UACC(NONE) OWNER(ADMIN)
AUDIT(FAILURE(READ))
PERMIT prefix.ACTIVATE CLASS(OPERCMDS) ACCESS(UPDATE) ID(syspautd)
```

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17452
 Group Title: ZB000030
 Rule ID: SV-46211r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZMIMR030
 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.

Responsibility: Information Assurance Officer
 IAControls: ECCD-1, ECCD-2

Check Content:

a) From the Administrator main menu, select 3;4 (Security Server Reports - General Resource Reports) and press ENTER.

b) Type 1 for General Resource Profile Summary and Tab down to CLASS: , type STARTED for class name.

c) Find the CA MIM General Resource profile. If not found go to step k. below.

d). Find the userid associated with the CA MIM started task under the STDATA segment information of the CA MIM general resource profile.

e). Go back to Administrator main menu, select 3;1 (Security Server Reports User Profile) and press ENTER.

f) Tab down to User ID and enter the User ID found in Step d) above and hit enter.

g). Page down till the Attributes section of the profile.

h) Verify that Protected = Yes .

i) If Protected = Yes, there is no FINDING.

j). If Protected = No, there is a FINDING.

k) If CA MIM is NOT found as a General Resource profile under the STARTED class in c. above, then check if is defined in the Started Procedures Table (ICHRIN03) as follows:

1, From Analyzer main Menu, go to 3;4 (Online Displays Started Procedures Analysis) and press ENTER.

2. Look for STARTED in the Source column and CAMIM in the Procname column.

3. If the CAMIM started procedure does not have an R in the M column there is NO FINDING (an R in the M column indicates that either the STARTED TASK USER ID does not have the protected attribute or is not defined (these are both findings)).

4. If there is an R in the M column, there is 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.

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):

```
au MIMGR name('STC, CA MIM') owner(stc) dfltgrp(stc) nopass
    data('CA MIM')
```

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-46213r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZMIMR032
Rule Title: CA MIM Resource Sharing Started task will be properly defined to the STARTED resource class for RACF.

Vulnerability Discussion: Access to product resources should be restricted to only those individuals responsible for the application connectivity and who have a requirement to access these resources. Improper control of product resources could potentially compromise the operating system, ACP, and customer data.

Responsibility: Information Assurance Officer
IAControls: ECCD-1, ECCD-2

Check Content:

a) From the Administrator main menu, select 3;4 (Security Server Reports - General Resource Reports) and press ENTER.

b) Type 1 for General Resource Profile Summary and tab down to CLASS and enter 'STARTED' for class name.

c) Find the CA MIM started task procname.

d). If found, there is NO FINDING.

e) If not found, then check if is defined in the Started Procedures Table (ICHRIN03)

as follows:

1. From Analyzer main Menu, go to 3;4 (Online Displays Started Procedures Analysis) and Press Enter.
2. Look for STARTED in the Source column and the CA MIM started task proc name in the Procname column
3. If found, there is NO FINDING.
4. If it is not found, there is 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 userid must be assigned for the CA MIM Resource Sharing started task(s) thru a corresponding STARTED class entry.

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

```
rdef started MIMGR.** uacc(none) owner(admin) audit(all(read))
      stdata(user(MIMGR) group(stc))
setr racl(started) ref
```

CCI: CCI-000764

UNCLASSIFIED