VANGUARD
INTEGRITY PROFESSIONALS
INFORMATION SECURITY EXPERTS

z/OS CA MICS for RACF STIG

Version: 6

Release: 4

8 July 2015

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

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-49858r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZMICR000
Rule Title: CA MICS Resource Management installation data sets must be properly protected.

Vulnerability Discussion: CA MICS Resource Management 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
IAControls: 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 MICS resource management installation datasets (they may possibly be called or begin with SYS2.MICS).

b) Ensure the following data set controls are in effect for the CA-MICS resource management installation data sets:

- READ access to the CA MICS installation data sets is restricted to authorized users (i.e. auditors, security administrators, and MICS end users).

- UPDATE or higher access to the CA MICS installation data sets is restricted to systems programming personnel and MICS administrators.

- UACC (None) and NOWARNING are specified for the CA MICS installation data sets.

- The RACF data set rules for the CA MICS 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 MICS 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 Update' 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 Update' which means that all failed UPDATE access is logged as specified in b. above.

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

d) If UPDATE access or higher to the CA MICS installation data sets are restricted to systems programming personnel, there is NO FINDING.

e) If UPDATE access or higher to the CA MICS installation data sets are not restricted to systems programming personnel there is a FINDING.

f) If UACC = None and Warning = No for all the CA MICS installation data sets there is NO FINDING.

g) If UACC is not None or Warning is not No for all the CA MICS installation data sets, there is a FINDING.

h) If all accesses of UPDATE or higher are logged for all the CA MICS installation data sets there is NO FINDING.

i) If all accesses of UPDATE or higher are not logged for all the CA MICS installation data sets, there is a FINDING.

Fix Text: The IAO will ensure UPDATE and/or greater access to CA MICS Resource Management installation data sets is limited to System Programmers and MICS administrators. READ access can be given to all authorized users (e.g., auditors, security administrators, and MICS end users). All failures and successful UPDATE 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 UPDATE and/or greater access and, if required, that all UPDATE and/or greater access is logged. He will identify if any additional groups have UPDATE 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.MICS.

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

```
ad 'SYS2.MICS.**' uacc(none) owner(sys2) -
       audit(success(update) failures(read)) -
      data('CA-MICS Resource Management Install DS')
pe 'SYS2.MICS.**' id(syspaudt tstcaudt micsadm) acc(a)
pe 'SYS2.MICS.**' id(audtaudt micsuser secaaudt) acc(r)

setr generic(dataset) refresh
```

CCI: CCI-000213

CCI: CCI002234

Group ID (Vulid): V-21592
Group Title: ZB000002
Rule ID: SV-50081r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZMICR002
Rule Title: CA MICS Resource Management User data sets must be properly protected.

Vulnerability Discussion: CA MICS Resource Management User 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
IAControls: 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 MICS resource management user datasets (they may possibly be called or begin with SYS2.MICS.DATA).

b) Ensure the following data set controls are in effect for the CA-MICS resource management user data sets:

- READ access to the CA MICS user data sets is restricted to authorized users (i.e. auditors, security administrators, MICS end users).

- WRITE or higher access to the CA MICS user data sets is restricted to systems programming personnel, SMF Batch user(s) and MICS Administrators.

- UACC (None) and NOWARNING are specified for the CA MICS user data sets.

- The RACF data set rules for the CA MICS user data sets specify that all accesses of WRITE 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 MICS 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 WRITE 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 WRITE access is logged as specified in b. above.
7. Repeat steps 1-6 above for any other CA MICS dataset profiles.

d) If WRITE access or higher to the CA MICS user data sets are restricted to systems programming personnel, there is NO FINDING.

e) If WRITE access or higher to the CA MICS user data sets are not restricted to systems programming personnel there is a FINDING.

f) If UACC = None and Warning = No for all the CA MICS user data sets there is NO FINDING.

g) If UACC is not None or Warning is not No for all the CA MICS user data sets, there is a FINDING.

h) If all accesses of WRITE or higher are logged for all the CA MICS user data sets there is NO FINDING.

i) If all accesses of UPDATE or higher are not logged for all the CA MICS user data sets, there is a FINDING.

Fix Text: The IAO will ensure WRITE and/or greater access to CA MICS Resource Management User data sets is limited to SMF Batch user(s), MICS Administrators, and systems programming personnel. READ access can be given to all authorized users (e.g., auditors, security administrators, and MICS end 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 (additional data sets may be required): SYS2.MICS.DATA.

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

```
ad 'SYS2.MICS.DATA.**' uacc(none) owner(sys2) -
       audit(failures(read)) -
      data('Vendor DS Profile: Product')
pe 'SYS2.MICS.DATA.**' id(syspaudt tstcaudt micsadm smfbaudt) acc(a)
pe 'SYS2.MICS.DATA.**' id(audtaudt micsuser secaaudt) acc(r)

setr generic(dataset) refresh
```

CCI: CCI-001499

UNCLASSIFIED