VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

# z/OS CA MICS for TSS STIG

## Version: 6

## Release: 4

## 26 Jul 2019

XSL Release 1/29/2015 Sort by: STIGID

---

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-49525r3_rule
Severity: CAT II
Rule Version (STIG-ID): ZMICT000
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.

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(MICSRPT)

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

- PDI(ZMIC0000)

Verify that the accesses to the CA-MICS Resource Management installation 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 all authorized users (e.g., auditors, security administrators, and MICS end 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 MICS administrators.

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

Fix Text: The IAO will ensure WRITE 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 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.MICS.

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

TSS PERMIT(syspaudt) DSN(SYS2.MICS) ACCESS(R)
TSS PERMIT(syspaudt) DSN(SYS2.MICS) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(tstcaudt) DSN(SYS2.MICS) ACCESS(R)
TSS PERMIT(tstcaudt) DSN(SYS2.MICS) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(micsadm) DSN(SYS2.MICS) ACCESS(R)
TSS PERMIT(micsadm) DSN(SYS2.MICS) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(audtaudt) DSN(SYS2.MICS) ACCESS(R)
TSS PERMIT(micsuser) DSN(SYS2.MICS) ACCESS(R)
TSS PERMIT(secaaudt) DSN(SYS2.MICS) ACCESS(R)

CCI: CCI-000213

CCI: CCI-002234

---

Group ID (Vulid): V-21592
Group Title: ZB000002
Rule ID: SV-50082r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZMICT002
Rule Title: CA MICS Resource Management User data sets must be properly protected.

Vulnerability Discussion: CA MICS Resource Management User datasets contain

sensitive data obtained through the MICS data collection process. Failure to properly identify and restrict access to these data sets could result in unauthorized access to sensitive data.

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

- SENSITVE.RPT(MICSUSER)

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

- PDI(ZMIC0002)

Verify that the accesses to the CA MICS Resource Management User 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 all authorized users (e.g., auditors, security administrators, and MICS end 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 SMF Batch user(s) and MICS Administrators.

___ The TSS data set access authorizations restrict WRITE and/or greater access to SMF Batch user(s) and MICS Administrators.

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:

```
TSS PERMIT(syspaudt) DSN(SYS2.MICS.DATA.) ACCESS(ALL)
TSS PERMIT(tstcaudt) DSN(SYS2.MICS.DATA.) ACCESS(ALL)
TSS PERMIT(micsadm) DSN(SYS2.MICS.DATA.) ACCESS(ALL)
TSS PERMIT(smfbaudt) DSN(SYS2.MICS.DATA.) ACCESS(ALL)
TSS PERMIT(audtaudt) DSN(SYS2.MICS.DATA.) ACCESS(R)
TSS PERMIT(micsuser) DSN(SYS2.MICS.DATA.) ACCESS(R)
TSS PERMIT(secaaudt) DSN(SYS2.MICS.DATA.) ACCESS(R)
```

CCI: CCI-000213

---