



z/OS BMC CONTROL-M/Restart for TSS STIG

Version: 6

Release: 5

23 Oct 2015

Group ID (Vulid): V-16932

Group Title: ZB000000

Rule ID: SV-31829r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZCTRT000

Rule Title: BMC CONTROL-M/Restart installation data sets will be properly protected.

Vulnerability Discussion: BMC CONTROL-M/Restart 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:

- SENSITIVE.RPT(CTRRPT)

Automated Analysis

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

- PDI(ZCTR0000)

Verify that the accesses to the BMC CONTROL-M/Restart 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 auditors, BMC users, and BMC STCs and/or batch users.

___ The TSS data set access authorizations restrict 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 BMC CONTROL-M/Restart installation data sets are limited to System Programmers only, and all WRITE and/or greater access is logged. READ access can be given to auditors, BMC users, and BMC STCs and/or batch 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 update and alter access and if required that all update and allocate access is logged. He will identify if any additional groups have update and/or alter 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.IOA.*.CTRO.

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

```
TSS PERMIT(<sypaudt>) DSN(SYS2.IOA.*.CTRO.) ACCESS(R)
TSS PERMIT(<sypaudt>) DSN(SYS2.IOA.*.CTRO.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<audtaudt>) DSN(SYS2.IOA.*.CTRO.) ACCESS(R)
TSS PERMIT(<bmcuser>) DSN(SYS2.IOA.*.CTRO.) ACCESS(R)
TSS PERMIT(CONTROLR) DSN(SYS2.IOA.*.CTRO.) ACCESS(R)
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-21592
Group Title: ZB000002
Rule ID: SV-32220r4_rule
Severity: CAT II
Rule Version (STIG-ID): ZCIRT002
Rule Title: BMC CONTROL-M/Restart Archived Sysout data sets must be properly protected.

Vulnerability Discussion: BMC CONTROL-M/Restart Archived Sysout 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.

IACControls: 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:

- SENSITIVE.RPT(CTRUSER)

Automated Analysis

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

- PDI(ZCTR0002)

Verify that the accesses to the BMC CONTROL-M/Restart Archived Sysout 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 BMC users.

___ The TSS data set access authorizations restrict WRITE and/or greater access to Production Control Scheduling personnel, scheduled batch user(s), systems programming personnel, and the BMC STCs and/or batch users.

Fix Text: Ensure that WRITE and/or greater access to BMC CONTROL-M/Restart Archived Sysout data sets are limited to production control scheduling personnel, scheduled batch users, System Programmers, and the BMC STCs and/or batch users only. READ access can be given to auditors and BMC users.

The installing Systems Programmer will identify and document the product data sets and categorize them according to who will have update and alter access and if required that all update and allocate access is logged.

The installing Systems Programmer will identify if any additional groups have update and/or alter access for specific data sets, and once documented 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:
CTRSYS.

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

TSS PERMIT(<syspautd>) DSN(CTRSYS.) ACCESS(ALL)

TSS PERMIT(CONTROLM) DSN(CTRSYS.) ACCESS(ALL)
TSS PERMIT(CONTDAY) DSN(CTRSYS.) ACCESS(ALL)
TSS PERMIT(<audtaudt>) DSN(CTRSYS.) ACCESS(READ)
TSS PERMIT(<bmcuser>) DSN(CTRSYS.) ACCESS(READ)
TSS PERMIT(<autoaudt>) DSN(CTRSYS.) ACCESS(ALL)
TSS PERMIT(<pcspaudt>) DSN(CTRSYS.) ACCESS(ALL)

CCI: CCI-000213

UNCLASSIFIED