VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

# z/OS BMC CONTROL-M for TSS STIG

Version: 6

Release: 9

25 Oct 2019

XSL Release 1/29/2015 Sort by: STIGID

Group ID (Vulid): V-17985
Group Title: ZB000060
Rule ID: SV-32017r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTM0060
Rule Title: BMC CONTROL-M security exits are not installed or configured properly.

Vulnerability Discussion: The BMC CONTROL-M security exits enable access authorization checking to BMC CONTROL-M commands, features, and online functionality. If these exit(s) is (are) not in place, activities by unauthorized users may result. BMC CONTROL-M security exit(s) interface with the ACP. If an unauthorized exit was introduced into the operating environment, system security could be weakened or bypassed. These exposures may result in the compromise of the operating system environment, ACP, and customer data.

Check Content:
Interview the systems programmer responsible for the BMC CONTROL-M. Determine if the site has modified the following security exit(s):

CTMSE01
CTMSE02
CTMSE08

Ensure the above security exit(s) has (have) not been modified.

If the above security exit(s) has (have) been modified, ensure that the security exit(s) has (have) been approved by the site systems programmer and the approval is on file for examination.

Fix Text: The System programmer responsible for the BMC CONTROL-M will review the BMC CONTROL-M operating environment. Ensure that the following security exit(s) is (are) installed properly. Determine if the site has modified the following security exit(s):

CTMSE01
CTMSE02
CTMSE08

Ensure that the security exit(s) has (have) not been modified.

If the security exit(s) has (have) been modified, ensure the security exit(s) has (have) been checked as to not violate any security integrity within the system and approval documentation is on file.

CCI: CCI-000035

---

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-31899r3_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTMT000
Rule Title: BMC CONTROL-M installation data sets will be properly protected.

Vulnerability Discussion: BMC CONTROL-M 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.

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

- SENSITVE.RPT(CTMRPT)

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

- PDI(ZCTM0000)

Verify that the accesses to the BMC CONTROL-M 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, automated operations, BMC users, operations, production control and scheduling personnel (domain level and decentralized), 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 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, automated operations, BMC users, operations, production control and scheduling personnel

(domain level and decentralized), 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.*.CTMI.

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

TSS PERMIT(<syspaudt>) DSN(SYS2.IOA.*.CTMI.) ACCESS(R)
TSS PERMIT(<syspaudt>) DSN(SYS2.IOA.*.CTMI.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<audtaudt>) DSN(SYS2.IOA.*.CTMI.) ACCESS(R)
TSS PERMIT(<autoaudt>) DSN(SYS2.IOA.*.CTMI.) ACCESS(R)
TSS PERMIT(<bmcuser>) DSN(SYS2.IOA.*.CTMI.) ACCESS(R)
TSS PERMIT(<dpcsaudt>) DSN(SYS2.IOA.*.CTMI.) ACCESS(R)
TSS PERMIT(<operaudt>) DSN(SYS2.IOA.*.CTMI.) ACCESS(R)
TSS PERMIT(<pcspaudt>) DSN(SYS2.IOA.*.CTMI.) ACCESS(R)
TSS PERMIT(CONTROLM) DSN(SYS2.IOA.*.CTMI.) ACCESS(R)

CCI: CCI-000213

CCI: CCI-002234

---

Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-31942r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTMT001
Rule Title: BMC CONTROL-M STC data sets will be properly protected.

Vulnerability Discussion: BMC CONTROL-M 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.

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

- SENSITVE.RPT(CTMSTC)

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

- PDI(ZCTM0001)

Verify that the accesses to the BMC CONTROL-M STC 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 auditors and BMC users.

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

___ The TSS data set access authorizations restricts UPDATE access to the BMC STCs and/or batch users.

___ The TSS data set access authorizations restricts UPDATE access to scheduled batch jobs, operations, and production control and scheduling personnel.

Fix Text: The IAO will ensure that WRITE and/or greater access to BMC CONTROL-M STC data sets are limited to System Programmers only. UPDATE access can be given to scheduled batch jobs, operations, and production control and scheduling personnel, BMC STCs and/or batch users. READ access can be given to auditors and/or 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. 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:
SYS3.IOA.*.CTMO.

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

TSS PERMIT(<syspaudt>) DSN(SYS3.IOA.*.CTMO.) ACCESS(ALL)
TSS PERMIT(<tstcaudt>) DSN(SYS3.IOA.*.CTMO.) ACCESS(ALL)
TSS PERMIT(CONTDAY) DSN(SYS3.IOA.*.CTMO.) ACCESS(U)
TSS PERMIT(CONTROLM) DSN(SYS3.IOA.*.CTMO.) ACCESS(U)
TSS PERMIT(<autoaudt>) DSN(SYS3.IOA.*.CTMO.) ACCESS(U)
TSS PERMIT(<operaudt>) DSN(SYS3.IOA.*.CTMO.) ACCESS(U)
TSS PERMIT(<pcspaudt>) DSN(SYS3.IOA.*.CTMO.) ACCESS(U)
TSS PERMIT(<audtaudt>) DSN(SYS3.IOA.*.CTMO.) ACCESS(R)
TSS PERMIT(<bmcuser>) DSN(SYS3.IOA.*.CTMO.) ACCESS(R)

CCI: CCI-001499

---

Group ID (Vulid): V-21592
Group Title: ZB000002
Rule ID: SV-32161r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTMT002
Rule Title: BMC CONTROL-M User data sets will be properly protected.

Vulnerability Discussion: BMC CONTROL-M User data sets, Repository, 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.

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

- SENSITVE.RPT(CTMUSER)

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

- PDI(ZCTM0002)

Verify that the accesses to the BMC CONTROL-M 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 auditors.

___ 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 BMC STCs and/or batch users.

___ The TSS data set access authorizations restrict UPDATE access to the BMC Users, operations, and production control and scheduling personnel (both domain level and Application level).

Fix Text: The IAO will ensure that WRITE and/or greater access to BMC CONTROL-M User data sets are limited to System Programmers and/or BMC STCs and/or batch users only. UPDATE access can be given to the BMC Users, operations, and production control and scheduling personnel (both domain level and Application level). READ access can be given to auditors.

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:
SYS3.IOA.*.CTMC.

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

TSS PERMIT(<syspaudt>) DSN(SYS3.IOA.*.CTMC.) ACCESS(ALL)
TSS PERMIT(BMC STCs) DSN(SYS3.IOA.*.CTMC.) ACCESS(ALL)
TSS PERMIT(<bmcuser>) DSN(SYS3.IOA.*.CTMC.) ACCESS(UPDATE)
TSS PERMIT(<operaudt>) DSN(SYS3.IOA.*.CTMC.) ACCESS(UPDATE)
TSS PERMIT(<pcspaudt>) DSN(SYS3.IOA.*.CTMC.) ACCESS(UPDATE)
TSS PERMIT(<dpcsaudt>) DSN(SYS3.IOA.*.CTMC.) ACCESS(UPDATE)
TSS PERMIT(<audtaudt>) DSN(SYS3.IOA.*.CTMC.) ACCESS(READ)

CCI: CCI-000213

---

Group ID (Vulid): V-17072
Group Title: ZB000003
Rule ID: SV-32217r4_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTMT003
Rule Title: BMC CONTROL-M User/Application JCL data sets must be properly protected.

Vulnerability Discussion: BMC CONTROL-M User/Application JCL 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.

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

- SENSITVE.RPT(CTMJCL)

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

- PDI(ZCTM0003)

Verify that the accesses to the BMC CONTROL-M User/Application JCL data sets are limited to only those who require access to perform their job duties. If the following guidance is true, this is not a finding.

___ The TSS data set access authorizations restrict READ access to auditors, automated batch user(s), BMC user(s), and operations.

___ The TSS data set access authorizations restrict WRITE and/or greater access to BMC CONTROL-M administrators and systems programming personnel.

___ The TSS data set access authorizations restrict UPDATE access to the Production Control and Scheduling personnel (both domain level and Application level) and BMC STCs and/or batch users. Accesses must be reviewed and approved by the IAO based on a documented need to perform job duties. Application (external users) will not have access to internal/site data sets.

Note: Update or greater access of the site's DASD Administrator Batch Processing

JCL and Procedures must be limited to only the LPAR level DASD Administrators. Update or greater access of the site's (LPAR Level) IA (Security) administrative batch processing JCL and Procedures must be limited to only the LPAR LEVEL ISSO/ISSM Team. It is recommended that multiple data sets be created, one of which that contains JCL and Procedures that are considered restricted and this data set be authorized to those user with justification to maintain and run these restricted JCL and Procedures.

Fix Text: Ensure that WRITE and/or greater access to BMC CONTROL-M User/Application JCL data sets are limited to System Programmers and/or BMC administrators only. UPDATE access can be given to the production control and scheduling personnel (both domain level and Application level) and BMC STCs and/or batch users. READ access can be given to auditors, automated batch user(s), BMC users, and operations. Access will be based on a documented need to know requirement. Application (external users) will not have access to internal/site data sets.

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:
IOA.

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

TSS PERMIT(<bmcadmin>) DSN(IOA.) ACCESS(ALL)
TSS PERMIT(<syspaudt>) DSN(IOA.) ACCESS(ALL)
TSS PERMIT(<tstcaudt>) DSN(IOA.) ACCESS(ALL)
TSS PERMIT(CONTDAY) DSN(IOA.) ACCESS(UPDATE)
TSS PERMIT(CONTROLM) DSN(IOA.) ACCESS(UPDATE)
TSS PERMIT(dpcsaudt) DSN(IOA.) ACCESS(UPDATE)
TSS PERMIT(<pcspaudt>) DSN(IOA.) ACCESS(UPDATE)
TSS PERMIT(<audtaudt>) DSN(IOA.) ACCESS(READ)
TSS PERMIT(<autoaudt>) DSN(IOA.) ACCESS(READ)
TSS PERMIT(<bmcuser>) DSN(IOA.) ACCESS(READ)
TSS PERMIT(<operaudt>) DSN(IOA.) ACCESS(READ)

CCI: CCI-000035

---

Group ID (Vulid): V-17947
Group Title: ZB000020
Rule ID: SV-32060r4_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTMT020
Rule Title: BMC C0NTROL-M resources must be properly defined and protected.

Vulnerability Discussion: BMC CONTROL-M 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.

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

- SENSITVE.RPT(ZCTM0020)

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

- PDI(ZCTM0020)

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

Note: To determine what resource class is used review the IOACLASS setting in SECPARM. The "Trigger" resources i.e., $$SECxxx (xxx is unique to the product) are defined in the FACILITY resource class

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

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

___ The TSS resource logging requirements are specified.

Fix Text: Verify that the following are properly specified in the ACP.

Note: To determine what resource class is used review the IOACLASS setting in SECPARM. The "Trigger" resources i.e., $$SECxxx (xxx is unique to the product) are defined in the FACILITY resource class

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

Use BMC CONTROL-M Resources and BMC INCONTROL Resources Descriptions tables in the zOS STIG Addendum. These tables list the resources, descriptions, and access and logging requirements. Ensure the guidelines for the resources and/or generic equivalent specified in the z/OS STIG Addendum are followed.

Note: It is the responsibility of the ISSM to determine and document appropriate personnel for access in accordance with DoD 8500.1 para 18(a),(b),(c).

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

TSS ADD(ADMIN) IOA($$CTMPNL3)
TSS PERMIT(BMC STCs) IOA($$CTMPNL3) ACC(ALL)
TSS PERMIT(<operaudt>) IOA($$CTMPNL3) ACC(ALL)
TSS PERMIT(<pcspaudt>) IOA($$CTMPNL3) ACC(ALL)
TSS PERMIT(<syspaudt>) IOA($$CTMPNL3) ACC(ALL)

CCI: CCI-000035

CCI: CCI-002234

---

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-32072r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTMT030
Rule Title: BMC CONTROL-M Started Task name is not properly identified / defined to the system ACP.

Vulnerability Discussion: BMC CONTROL-M 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.

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

- TSSCMDS.RPT(@ACIDS)

Review each BMC CONTROL-M STC/Batch ACID(s) for the following:

___ Defined with Facility of STC and/or BATCH.

___ Defined with Master Facility of CONTROLM.

___ Is sourced to the INTRDR.

Fix Text: The BMC CONTROL-M system programmer and the IAO will ensure that a product's Started Task(s) is properly Identified / 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.

A sample is provided here:

```
TSS CREATE(CONTROLM) TYPE(USER) -
     NAME('*STC* for IOA') DEPT(xxxx) -
    FAC(STC) -
    MASTFAC(CONTROLM) PASS(xxxxxxxx,0) -
    SOURCE(INTRDR) NOSUSPEND
```

CCI: CCI-000764

---

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-32158r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTMT032

Rule Title: BMC CONTROL-M Started task(s) must be properly defined to the Started Task Table ACID 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.

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(ZCTM0032)

Verify that the BMC CONTROL-M started task(s) is (are) defined in the TSS STC record.

Fix Text: The BMC CONTROL-M system programmer and the IAO will ensure that a product's started task(s) is (are) properly identified and/or defined to the System ACP.

A unique ACID must be assigned for the BMC CONTROL-M started task(s) thru a corresponding STC table entry.

The following sample set of commands is shown here as a guideline:

TSS ADD(STC) PROCNAME(CONTOLM) ACID(CONTROLM)

CCI: CCI-000764

---

Group ID (Vulid): V-17469
Group Title: ZB000036
Rule ID: SV-32051r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTMT036
Rule Title: BMC CONTROL-M is not properly defined to the Facility Matrix Table for Top Secret.

Vulnerability Discussion: Improperly defined security controls for the BMC CONTROL-M could result in the compromise of the network, operating system, and

customer data.

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

- TSSCMDS.RPT(FACLIST) - Preferred report containing all control option values in effect including default values
- TSSCMDS.RPT(TSSPRMFL) - Alternate report containing only control option values explicitly coded at TSS startup

Ensure the BMC CONTROL-M Facility Matrix table is defined as follows:

FAC(USERxx=NAME=CONTROLM,PGM=CTM,ID=nn,ACTIVE,SHRPRF)
FAC(CONTROLM=ASUBM,NOABEND,MULTIUSER,NOXDEF,SIGN(S))
FAC(CONTROLM=RES,LUMSG,STMSG,WARNPW,NORNDPW)
FAC(CONTROLM=NOAUDIT,NOTSOC,MODE=FAIL)
FAC(CONTROLM=LOG(SMF,INIT,MSG,SEC9),UIDACID=8,LOCKTIME=000)

Fix Text: The BMC CONTROL-M system programmer and the IAO will ensure that the TOP SECRET Facility Matrix Table is properly defined using the following example:

CONTROLM:
FAC(USERxx=NAME=CONTROLM,PGM=CTM,ID=nn,ACTIVE,SHRPRF)
FAC(CONTROLM=ASUBM,NOABEND,MULTIUSER,NOXDEF)
FAC(CONTROLM=LUMSG,STMSG,SIGN(S),WARNPW,NORNDPW)
FAC(CONTROLM=NOAUDIT,NOTSOC,MODE=FAIL)
FAC(CONTROLM=LOG(SMF,INIT,MSG,SEC9),UIDACID=8,LOCKTIME=000)

CCI: CCI-000764

---

Group ID (Vulid): V-18014
Group Title: ZB000040
Rule ID: SV-31980r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTMT040
Rule Title: BMC CONTROL-M configuration/parameter values must be specified properly.

Vulnerability Discussion: BMC CONTROL-M configuration/parameters control the security and operational characteristics of products. If these parameter values are improperly specified, security and operational controls may be weakened. This exposure may threaten the availability of the product applications, and compromise the confidentiality of customer data.

Check Content:
Refer to the following applicable reports produced by the z/OS Data Collection:

- IOA.RPT(SECPARM)

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

- PDI(ZCTM0040)

The following keywords will have the specified values in the BMC CONTROL-M security parameter member:

Keyword Value
DEFMCHKM $$CTMEDM
SECTOLM NO
DFMM01 EXTEND
DFMM02 EXTEND
DFMM08 EXTEND
TSSJCARD U
MSUBCHK NO

Fix Text: The BMC CONTROL-M Systems programmer will verify that any configuration/parameters that are required to control the security of the product are properly configured and syntactically correct. Set the standard values for the BMC CONTROL-M security parameters for the specific ACP environment along with additional IOA security parameters with standard values as documented below.

Keyword Value
DEFMCHKM $$CTMEDM
SECTOLM NO
DFMM01 EXTEND
DFMM02 EXTEND
DFMM08 EXTEND
TSSJCARD U
MSUBCHK NO

CCI: CCI-000035

---