

VANGUARD

Integrity Professionals, Inc.

Enterprise Security Software

z/OS BMC CONTROL-M for ACF2 STIG

Version: 6

Release: 9

29 Dec 2020

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.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, ECSD-1, ECSD-2

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-31898r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZCTMR000

Rule Title: BMC CONTROL-M installation data sets are not 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.

Responsibility: Information Assurance Officer

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(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 ACF2 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 ACF2 data set access authorizations restrict WRITE and/or greater access to systems programming personnel.

___ The ACF2 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 update and alter access to BMC CONTROL-M installation data sets is limited to System Programmers only, and all update and alter access is logged. Read access can be given to all authorized 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 alter 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.

Data sets to be protected will be:

SYS2.IOA.*.CTM*.**

SYS3.IOA.*.CTMI.**

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

```
ad 'SYS2.IOA.*.CTM*.**' uacc(none) owner(sys2) -  
  audit(success(update) failures(read)) -  
  data('BMC CONTROL-M Install DS')  
pe 'SYS2.IOA.*.CTM*.**' id(<syspau<dt>) acc(a)  
pe 'SYS2.IOA.*.CTM*.**' id(*) acc(r)  
ad 'SYS3.IOA.*.CTMI.**' uacc(none) owner(sys3) -  
  audit(success(update) failures(read)) -  
  data('BMC CONTROL-M Install DS')  
pe 'SYS3.IOA.*.CTMI.**' id(<syspau<dt>) acc(a)  
pe 'SYS3.IOA.*.CTMI.**' id(*) acc(r)
```

setr generic(dataset)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067

Group Title: ZB000001

Rule ID: SV-31941r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZCTMR001

Rule Title: BMC CONTROL-M STC data sets are not 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.

Responsibility: Information Assurance Officer

IACControls: DCSL-1, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:

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

- SENSITIVE.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 ACF2 data set access authorizations restricts READ access to auditors and BMC users.

___ The ACF2 data set access authorizations restricts WRITE and/or greater

access to systems programming personnel.

____ The ACF2 data set access authorizations restricts UPDATE access to the BMC STCs and/or batch users.

____ The ACF2 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 update and alter access to BMC CONTROL-M STC data sets is limited to System Programmers only. Update access can be given to scheduled batch jobs, operations, and production control and scheduling personnel, BMC CONTROL-M s STC(s), and/or batch user(s). Read access can be given to auditors and/or CONTROL-M end 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 alter 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.

Data sets to be protected will be:
SYS3.IOA.*.CTMO.**

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

```
ad 'SYS3.IOA.*.CTMO.**' uacc(none) owner(sys3) -  
  audit(failures(read)) -  
  data('BMC ControlM Started Task DS')  
pe 'SYS3.IOA.*.CTMO.**' id(<syspautd> <tstcaudt>) acc(a)  
pe 'SYS3.IOA.*.CTMO.**' id(CONTROLM CONTDAY <autoaudt> <operaudt> <pcspautd>)  
acc(u)
```

pe 'SYS3.IOA.*.CTMO.**' id(<audtaudt> <bmcuser>) acc(r)

setr generic(dataset) refresh

CCI: CCI-001499

Group ID (Vulid): V-21592

Group Title: ZB000002

Rule ID: SV-32160r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZCTMR002

Rule Title: BMC CONTROL-M User data sets are not 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.

Responsibility: Information Assurance Officer

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(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 ACF2 data set access authorizations restrict READ access to auditors.

___ The ACF2 data set access authorizations restrict WRITE and/or greater access to systems programming personnel.

___ The ACF2 data set access authorizations restrict WRITE and/or greater access to the BMC STCs and/or batch users.

___ The ACF2 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 update and allocate access to BMC CONTROL-M User data sets is limited to System Programmers and/or BMC CONTROL-M s STC(s) and/or batch user(s) only. Update access can be given to the Production Control and Scheduling personnel. 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.

Data sets to be protected will be:
SYS3.IOA.*.CTMC.**

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

controls:

```
ad 'SYS3.IOA.*.CTMC.**' uacc(none) owner(sys3) -  
    audit(failures(read)) -  
    data('ControlM Repository Dataset')  
pe 'SYS3.IOA.*.CTMC.**' id(<syspautd>) acc(a)  
pe 'SYS3.IOA.*.CTMC.**' id(<bmcuser> <operaudt> <pcspautd>) acc(a)  
pe 'SYS3.IOA.*.CTMC.**' id(CONTROLM CONTDAY) acc(a)  
pe 'SYS3.IOA.*.CTMC.**' id(<audtaudt>) acc(r)
```

setr generic(dataset) refresh

CCI: CCI-001499

Group ID (Vulid): V-17072

Group Title: ZB000003

Rule ID: SV-32216r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZCTMR003

Rule Title: BMC CONTROL-M User/Application JCL data sets are not 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.

Responsibility: Information Assurance Officer

IAControls: DCSL-1, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:

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

- SENSITIVE.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 ACF2 data set access authorizations restrict READ access to auditors, automated batch user(s), BMC user(s), and operations.

___ The ACF2 data set access authorizations restrict WRITE and/or greater access to BMC CONTROL-M administrators and systems programming personnel.

___ The ACF2 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 access of the site's DASD Administrator Batch Processing JCL and Procedures must be limited to only the LPAR level DASD Administrators. Update 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 users with justification to maintain and run these restricted JCL and

Procedures.

Fix Text: The IAO will ensure that update and alter access to BMC CONTROL-M User/Application JCL data sets are limited to BMC CONTROL-M administrators only. Update access can be given to the Production Control and Scheduling personnel and/or BMC CONTROL-M s STC(s) and/or BMC CONTROL-M s batch user(s). Read access can be given to auditors and automated batch user(s).

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 alter 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.

Data sets to be protected will be:

IOA.**

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

```
ad 'IOA.**' uacc(none) owner(IOA) -  
    data('ControlM User Datasets')  
pe 'IOA.**' id(<syspautd>) acc(a)  
pe 'IOA.**' id(<audtautd> <autoautd>) acc(r)  
pe 'IOA.**' id(<bmcuser> <bmcbatch> <operautd> <pcspautd>) acc(r)  
pe 'IOA.**' id(CONTROLM CONTDAY) acc(r)
```

setr generic(dataset) refresh

CCI: CCI-000035

Group ID (Vulid): V-17947

Group Title: ZB000020

Rule ID: SV-32059r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZCTMR020

Rule Title: BMC CONTROL-M resources are not 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.

Responsibility: Information Assurance Officer

IAControls: ECCD-1, ECCD-2

Check Content:

Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITVE.RPT(ZCTM0020)
- ACF2CMD5.RPT(RESOURCE) Alternate report

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 IOACCLASS setting in SECPARM. The "Trigger" resources i.e., \$\$SECxxx (xxx is unique to the product) are defined in the FACILITY resource class

___ The ACF2 resources are defined with a default access of PREVENT.

___ The ACF2 resource access authorizations restrict access to the appropriate personnel.

___ The ACF2 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 IOACCLASS 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:

```
$key($$ctmpnl3) type(ioa)
```

- uid(BMC STCs) allow
- uid(<operaudt>) allow
- uid(<pcspaudt>) allow
- uid(<syspaudt>) allow
- uid(*) prevent

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17452

Group Title: ZB000030

Rule ID: SV-32071r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZCTMR030

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.

Responsibility: Information Assurance Officer

IACControls: ECCD-1, ECCD-2

Check Content:

Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ATTSTC)

Insure that the logonids(s) for the BMC CONTROL-M started task(s) includes the following:

STC

MUSASS

NO-SMC

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:

```
au CONTROLM name('stc, BMC CONTROL-M') owner(stc) dfltgrp(stc) nopass
```

CCI: CCI-000764

Group ID (Vulid): V-18014

Group Title: ZB000040

Rule ID: SV-31979r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZCTMR040

Rule Title: BMC CONTROL-M configuration/parameter values are not 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.

Responsibility: Systems Programmer

IAControls: ECCD-1, ECCD-2

Check Content:

a) Ensure the following keywords are specified in the BMC CONTROL-M security parameter member:

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

b) If all of the above are specified in the BMC CONTROL-M SECPARM, there is NO FINDING.

c) If any of the abover are not specified in the BMC CONTROL-M SECPARM, there is a FINDING.

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
RACJCARD	U
MSUBCHK	NO

CCI: CCI-000035

UNCLASSIFIED