

# VANGUARD

## INTEGRITY PROFESSIONALS

---

### INFORMATION SECURITY EXPERTS

z/OS BMC CONTROL-M for RACF STIG

Version: 6

Release: 10

30 June 2023

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

---

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:

1. Check with your IOA or Systems Programming personnel and compile the list of

BMC CONTROL-M Installation Datasets, Most likely they are similar to:  
SYS2.IOA.\*.CTM\*.\* or SYS3.IOA.\*.CTMI.\*.

2. From the Administrator Main Menu Choose Option 2 Security Server Commands.

3. Then choose Option: 3 Data Set.

4. Type the resource names collected in option 1. above into: "Enter fully qualified (without quotes) data set or profile name: ".

5. Hit enter.

6. Enter Y for Display covering profile?

7. Verify that the UACC is NONE.

8. Verify that Audit Successes and Failures specifies UPDATE or READ.

9. Tab down to Standard Access Permits and place an E next to it (hit enter)and validate that UPDATE or higher access is limited to Systems Programming personnel. Verify Read access is given to:

- Auditors
- BMC Users
- Scheduling Personnel (both centralized and decentralized)
- BMC STCs
- Batch Users

10. If CONDITIONAL ACCESS PERMITS: \_ (E to edit data) has \*data is present\* next to it, place an E next to it and validate that conditional access

permits of Update or higher are limited to Systems Programming Personnel as

well. Verify Read access is given to:

- Auditors

- BMC Users
- Security Personnel (both centralized and decentralized)
- BMC STCs
- Batch Users

11. Repeat steps 2 through 10 for all datasets in option 1.above.

12 .If 7, 8, 9 and 10 are all true, there is NO FINDING.

13. If 7, 8, 9 and 10 are not true, this is a FINDING.

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

Check Content:

a) Check with your IOA or Systems Programming personnel and compile the list of BMC Control-M STC and/or batch data sets datasets, Most likely they are similar

to:

SYS3.IOA.\*.CTDO.\*\*.

1. From the Administrator Main Menu Choose Option 2 Security Server Commands.

2. then choose Option: 3 Data Set.

3. Type the resource names collected in option a.1 above into: "Enter fully qualified (without quotes) data set or profile name: ".

4. Hit enter.

5. Enter Y for Display covering profile?

6. Verify that the UACC is NONE.

7. Verify that Audit Successes and Failures specifies UPDATE or READ.

8. Tab down to Standard Access Permits and place an E next to it (hit enter).

Validate that UPDATE access or greater is limited to Systems Programming personnel. Verify that Scheduled Batch jobs, BMC STCs, Batch Users, Operations, Production Control and Scheduling personnel are permitted UPDATE access.

Verify Read Access is permitted to Auditors and BMC users.

9. If CONDITIONAL ACCESS PERMITS: \_ (E to edit data) has \*data is present\* next to it, place an E next to it and hit enter. Validate that UPDATE access or greater is limited to Systems Programming personnel. Verify that Scheduled Batch jobs, BMC STCs, Batch Users, Operations, Production Control and Scheduling personnel are permitted UPDATE access. Verify Read Access is permitted to Auditors and BMC users.
10. Repeat steps 1 through 9 for all datasets in option a). above.
11. If 6, 7, 8, and 9 are all true, there is NO FINDING.
12. If 7, 8, 9 and 10 are not true, this is a FINDING.

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(<syspau> <tstcaudt>) acc(a)
pe 'SYS3.IOA.*.CTMO.**' id(CONTROLM CONTDAY <autoaudt> <operaudt>
<pcspau>)
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:

1. Check with your IOA or Systems Programming personnel and compile the list of

CONTROL-M user data sets, Most likely they are similar to:

SYS3.IOA.\*.CTDR.\*\*

CTRUSR.\*\*

CTDSRV.\*\*

CTDJB1.\*\*

2. From the Administrator Main Menu Choose Option 2 Security Server Commands.

3. Then choose Option: 3 Data Set.

4. Type the resource names collected in option 1 above into: "Enter fully qualified (without quotes) data set or profile name:".

5. Hit enter.

6. Enter Y for Display covering profile?

7. Verify that the UACC is NONE.

8. Verify that Audit Successes and Failures specifies UPDATE or READ.

9. Tab down to Standard Access Permits and place an E next to it (hit enter).

Validate that UPDATE access or greater is limited to Systems Programming personnel. Verify that BMC STCs, Batch users.

BMC Users, Operations, Production Control and Scheduling personnel are permitted

UPDATE access.

Verify Read Access is permitted to Auditors.

10. if CONDITIONAL ACCESS PERMITS: \_ (E to edit data) has \*data is present\* next to it, place an E next to it and hit enter.  
 Validate that UPDATE access or greater is limited to Systems Programming personnel. Verify that BMC STCs, Batch users, BMC Users, Operations, Production Control and Scheduling personnel are permitted  
 UPDATE access.  
 Verify Read Access is permitted to Auditors.

11. Repeat steps 2 through 10 for all datasets in option 1. above.

12. If 7, 8, 9 and 10 are all true, there is NO FINDING.

13. If 7, 8, 9 and a.10 are not true, this is a FINDING.

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:

1. Check with your IOA or Systems Programming personnel and compile the list of BMC CONTROL-M User/Application JCL, Likely: called something like. IOA.\*\*.
2. From the Administrator Main Menu Choose Option 2 Security Server Commands
3. then choose Option: 3 Data Set
4. Type the resource names collected in option a.1 above into: Enter fully qualified (without quotes) data set or profile name:

- 
5. Hit enter.
  6. Enter Y for Display covering profile? Y
  7. Verify that the UACC is NONE
  8. Verify that Audit Successes and Failures specifies UPDATE or READ.
  9. Tab down to Standard Access Permits and place an E next to it (hit enter).
- Validate that UPDATE or higher access is limited to BMC CONTROL-M administrators and Systems Programmers and UPDATE access is permitted to Production Control and Scheduling personnel, BMC STCs, and/or the product's batch users. Verify READ access is permitted to auditors, automated batch users, BMC users and Operations Personnel
10. if CONDITIONAL ACCESS PERMITS: \_ (E to edit data) has \*data is present\* next to it, place an E next to it.
- Validate that UPDATE or higher access is limited to BMC CONTROL-M administrators and Systems Programmers and UPDATE access is permitted to Production Control and

Scheduling personnel, BMC STCs, and/or the product's batch users. Verify  
 READ  
 access is permitted to auditors, automated batch users, BMC users and  
 Operations  
 Personnel

11. Repeat steps 2 through 10 for all datasets in option 1

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(<syspau>) acc(a)
pe 'IOA.**' id(<audtaudt> <autoaudt>) acc(r)
pe 'IOA.**' id(<bmcuser> <bmcbatch> <operaudt> <pcspau>) 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:

Verify that the accesses to resources in the BMC CONTROL-M Resources table in the z/OS STIG Addendum are properly restricted.

Note: To determine what resource class is used review the IOAClass setting in SECPARM to determine the resource class to use. Refer to ZIOA0040 for this setting.

a) Verify the resources identified in the BMC CONTROL-M Resources table in the z/OS STIG Addendum are properly defined and access is restricted to the appropriate personnel.

For all the PROFILES found in BMC CONTROL-M Resources table in the z/OS STIG

Addendum:

1. From the Administrator Main Menu Chose Option 3 Security Server Reports
2. then chose Option: 4 General Resource Profile
3. On the command line chose option 4 AND then Put (\* or \$\$\*) next to PROFILE: and (class name from ZIOA0040) next to CLASS:

Profile: from table (or specify \$\$\* as all profile start with a \$\$)  
Class: from ZIOA0040

4. Hit enter.
5. Verify that the UACC for all profiles listed is NONE
6. Place an S next to the profile and validate that the access list is appropriate (as defined or more restrictive than the BMC CONTROL-M Resources table in the z/OS STIG Addendum.
7. If TYPE is GROUP, place an S in the CMD line and hit enter to explode the GROUP.

8.. For all resources with logging requirements place an LR next to the profile  
(hit  
enter and review the output) and validate that it specifies ALL(READ).

b) If all profiles, access lists, and Auditing are defined like or more restrictive than the  
BMC CONTROL-M Resources table in the z/OS STIG Addendum, then there is NO  
FINDING.

c) If any Profile, Access list or Auditing is more permissive than the  
BMC  
CONTROL-M Resources table in the z/OS STIG Addendum,  
then there is a FINDING.

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.

(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:

```
rdef $ioa $$ctmpnl3.** uacc(none) owner(admin)
  audit(failure(read)) -
  data('protected per zctmr020')

pe $$ctmpnl3.** cl($ioa) id(BMC STCs) acc(alter)
pe $$ctmpnl3.** cl($ioa) id(<operaudt>) acc(alter)
pe $$ctmpnl3.** cl($ioa) id(<pcspaadt>) acc(alter)
pe $$ctmpnl3.** cl($ioa) id(<syspaadt>) acc(alter)
```

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  
 IAControls: ECCD-1, ECCD-2

#### Check Content:

- a) From Analyzer main Menu, go to 3;4; Press ENTER
- b) Key in SORT PROCNAME; Press ENTER
- c) Key in L CONTROLM; Press ENTER
- d) If not found then CONTROLM; is not defined to RACF as a STC user.
- e) If found then use the U line command to determine if the userid is defined to RACF.
- f) The userid is defined to RACF if a userid display appears. If not defined you should see the message No data to display.
- g) now press f3 to go back to the previous display. If no R is next to the entry then the user is protected.
- h) If an R is next to the entry, place an M on the command line and validate the following is NOT displayed:  
 VSA346R The user ID does not have the protected attribute.
- i) If the userid for the CONTROL-M started task is defined to the security database and is protected, there is NO FINDING.
- j) If the userid for the CONTROL-M started task is not defined to the security database, or is defined but does not have the protected attribute,

this is a FINDING.

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-17454  
Group Title: ZB000032  
Rule ID: SV-32157r1\_rule  
Severity: CAT II  
Rule Version (STIG-ID): ZCTMR032  
Rule Title: BMC CONTROL-M Started task is not properly defined to the STARTED resource class for RACF.

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.

Responsibility: Information Assurance Officer  
IAControls: ECCD-1, ECCD-2

Check Content:

1. From Analyzer main Menu, go to 3;4; Press ENTER
2. Key in SORT PROCNAME; Press ENTER
3. Key in L CONTROLM or the name of the CONTROLM started task; Press ENTER
4. Look at the source column. It will indicate STARTED class profile or ICHRIN03 entry.

5. If not found then the CONTROLM started task is not defined to RACF as a STC user.

b) If a STARTED resource class profile exists for the CONTROLM STC, there is NO FINDING.

c) If neither a STARTED resource class profile or an ICHRIN03 entry exists for the CONTROLM STC, this is a FINDING.

b) If a STARTED resource class profile exists for the CONTROLM STC, there is NO FINDING.

c) If neither a STARTED resource class profile or an ICHRIN03 entry exists for the CONTROLM STC, this is a FINDING.

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.

A unique userid must be assigned for the ControlM started task thru a corresponding STARTED class entry.

A sample set of commands is shown here:

```
rdef started CONTROLM.** uacc(none) owner(admin) audit(all(read))
stdat(user(CONTROLM) group(stc))
setr racl(started) ref
```

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