

# **VANGUARD**

## **Integrity Professionals, Inc.**

---

### **Enterprise Security Software**

zOS BMC CONTROL-O for ACF2 STIG

Version: 6

Release: 7

29 Dec 2020

---

Group ID (Vulid): V-18014  
Group Title: ZB000040  
Rule ID: SV-32004r1\_rule  
Severity: CAT II  
Rule Version (STIG-ID): ZCTO0040  
Rule Title: BMC CONTROL-O configuration/parameter values are not specified properly.

Vulnerability Discussion: BMC CONTROL-O 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:  
Ensure the following keywords are specified in the BMC CONTROL-O security parameter member:

Keyword	Value
DEFMCHKO	\$\$CTOEDM
SECTOLO	NO
DFMO01	EXTEND
DFMO02	EXTEND
DFMO03	EXTEND
DFMO04	EXTEND
DFMO08	EXTEND
DFMO10	PROD (new for 6.3.xx)
DFMO15	EXTEND

Fix Text: The BMC CONTROL-O 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-O security parameters for the specific ACP environment along with additional IOA security parameters with standard values as documented below.

Keyword	Value
DEFMCHKO	\$\$CTOEDM
SECTOLO	NO
DFMO01	EXTEND
DFMO02	EXTEND
DFMO03	EXTEND
DFMO04	EXTEND
DFMO08	EXTEND
DFMO10	PROD (new for 6.3.xx)
DFMO15	EXTEND

CCI: CCI-000035

---

Group ID (Vulid): V-22689  
Group Title: ZB000041  
Rule ID: SV-32006r1\_rule  
Severity: CAT II  
Rule Version (STIG-ID): ZCTO0041  
Rule Title: BMC CONTROL-O configuration/parameter values are not specified properly.

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

Keyword	Value
RUNTDFT	OWNER
RUNTCACH	100
AUTOMLOG	V

Fix Text: The BMC CONTROL-O 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-O security parameters for the specific ACP environment along with additional IOA security parameters with standard values as documented below.

Keyword	Value
RUNTDFT	OWNER
RUNTCACH	100
AUTOMLOG	V

CCI: CCI-000035

---

Group ID (Vulid): V-17985  
Group Title: ZB000060  
Rule ID: SV-32016r1\_rule  
Severity: CAT II

Rule Version (STIG-ID): ZCTO0060

Rule Title: BMC CONTROL-O security exits are not installed or configured properly.

Vulnerability Discussion: The BMC CONTROL-O security exits enable access authorization checking to BMC CONTROL-O commands, features, and online functionality. If these exit(s) is (are) not in place, activities by unauthorized users may result. BMC CONTROL-O 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

IACControls: DCCS-1, DCCS-2, ECSD-1, ECSD-2

Check Content:

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

CTOSE01

CTOSE02

CTOSE03

CTOSE04

CTOSE08

CTOSE10

CTOSE15

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-O will review the BMC CONTROL-O operating environment. Ensure that the following security exit(s) is (are) installed properly. Determine if the site has modified the following security exit(s):

CTOSE01  
CTOSE02  
CTOSE03  
CTOSE04  
CTOSE08  
CTOSE10  
CTOSE15

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-31908r1\_rule

Severity: CAT II

Rule Version (STIG-ID): ZCTOR000

Rule Title: BMC CONTROL-O installation data sets are not properly protected.

Vulnerability Discussion: BMC CONTROL-O 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

IACControls: 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-O Installation Datasets. Most likely they are similar to SYS2.IOA.\*.CTO\*.\*\* or SYS3.IOA.\*.CTOI.\*\*.

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?

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 if applicable is given to:

Auditors

BMC Users

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 if applicable is given to:

Auditors

BMC Users

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-O installation data sets is limited to System Programmers only, and all update and allocate 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.\*.CTO\*.\*\*

SYS3.IOA.\*.CTOI.\*\*

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



```
ad 'SYS2.IOA.*.CTO*.*' uacc(none) owner(sys2) -  
  audit(success(update) failures(read)) -  
  data('Vendor DS Profile: BMC CONTROL-O')  
pe 'SYS2.IOA.*.CTO*.*' id(<syspau>) acc(a)  
pe 'SYS2.IOA.*.CTO*.*' id(<audtaudt> <bmcuser>)  
pe 'SYS2.IOA.*.CTO*.*' id(<CONTROLO> <bmcbatch>)  
pe 'SYS2.IOA.*.CTO*.*' id(*) acc(r)
```

```
ad 'SYS3.IOA.*.CTOI.*' uacc(none) owner(sys2) -  
  audit(success(update) failures(read)) -  
  data('Vendor DS Profile: BMC CONTROL-O')  
pe 'SYS3.IOA.*.CTOI.*' id(<syspau>) acc(a)  
pe 'SYS3.IOA.*.CTOI.*' id(<audtaudt> <bmcuser>)  
pe 'SYS3.IOA.*.CTOI.*' id(<CONTROLO> <bmcbatch>)  
pe 'SYS3.IOA.*.CTOI.*' id(*) acc(r)
```

setr generic(dataset) refresh

CCI: CCI-000213

CCI: CCI002234

---

Group ID (Vulid): V-17067  
Group Title: ZB000001  
Rule ID: SV-31944r1\_rule  
Severity: CAT II  
Rule Version (STIG-ID): ZCTOR001  
Rule Title: BMC CONTROL-O STC data sets are not properly protected.

Vulnerability Discussion: BMC CONTROL-O 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 Systems Security 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(CTOSTC)

Automated Analysis

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

- PDI(ZCTO0001)

Verify that the accesses to the BMC CONTROL-O STC 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, operators, and domain level production control and scheduling personnel.

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

\_\_\_ The ACF2 data set access authorizations restrict UPDATE access to the BMC users and BMC STCs and/or batch users.

Fix Text: The ISSO will ensure that UPDATE or higher access to BMC CONTROL-O STC

data sets is limited to System Programmers. UPDATE access can be given to BMC STC(s) and/or batch user(s). Read access can be given to Auditors, System Operators, and domain level Production Control and Scheduling personnel.

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 ISSO 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.\*.CTOO.\*\*

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

```
ad 'SYS3.IOA.*.CTOO.**' uacc(none) owner(sys3) -  
audit(failures(read)) -  
data('BMC CONTROL-O Operational & Respostory')  
pe 'SYS3.IOA.*.CTOO.**' id(<sypaudt>) acc(a)  
pe 'SYS3.IOA.*.CTOO.**' id(CONTROLO) acc(u)  
pe 'SYS3.IOA.*.CTOO.**' id(<bmcuser> <bmcbatch>) acc(u)  
pe 'SYS3.IOA.*.CTOO.**' id(<audtaudt>) acc(r)
```

setr generic(dataset) refresh

CCI: CCI-001499

---

Group ID (Vulid): V-17947

Group Title: ZB000020

Rule ID: SV-32062r1\_rule

Severity: CAT II

Rule Version (STIG-ID): ZCTOR020

Rule Title: BMC CONTROL-O resources are not properly defined and protected.

Vulnerability Discussion: BMC CONTROL-O 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(ZCTO0020)
- ACF2CMDS.RPT(RESOURCE) Alternate report

Automated Analysis

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

- PDI(ZCTO0020)

Verify that the accesses to resources and/or generic equivalent are properly restricted according to the requirements specified in BMC CONTROL-O 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: The IAO will work with the systems programmer to 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-O 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.

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

```
$key($$ctoap) type(ioa)  
- uid(<operaudt>) log
```

- uid(<pcspaudt>) log
- uid(<prodaudt>) log
- uid(<syspaudt>) log
- uid(\*) prevent

CCI: CCI-000035

CCI: CCI-002234

---

Group ID (Vulid): V-17452

Group Title: ZB000030

Rule ID: SV-32074r1\_rule

Severity: CAT II

Rule Version (STIG-ID): ZCTOR030

Rule Title: BMC CONTROL-O Started Task name is not properly identified / defined to the system ACP.

Vulnerability Discussion: BMC CONTROL-O 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:

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

- ACF2CMDS.RPT(ATTSTC)

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

STC  
MUSASS  
NO-SMC

Fix Text: The BMC CONTROL-O 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 CONTROL0 name('stc, BMC CONTROL-O') owner(stc) dfltgrp(stc) nopass

CCI: CCI-000764

---

UNCLASSIFIED