

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

z/OS BMC CONTROL-D for RACF STIG

Version: 6

Release: 8

30 June 2023

XSL Release 6/30/2023 Sort by: STIGID
Description:

Group ID (Vulid): V-18014
Group Title: ZB000040
Rule ID: SV-32211r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTD0040
Rule Title: BMC CONTROL-D configuration/parameter values are not specified properly.

Vulnerability Discussion: BMC CONTROL-D 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-D security parameter member:

Keyword	Value
DEFMCHKD	\$\$CTDEDM
SECTOLD	NO
DFMD01	EXTEND
DFMD04	EXTEND
DFMD08	EXTEND
DFMD19	EXTEND
DFMD23	EXTEND
DFMD24	EXTEND
DFMD26	EXTEND
DFMD27	EXTEND

b) If the keywords and values are as required above, there is NO FINDING.

c) If the keywords and values are NOT as required above, there is a FINDING.

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

Keyword	Value
DEFMCHKD	\$\$CTDEDM
SECTOLD	NO
DFMD01	EXTEND
DFMD04	EXTEND
DFMD08	EXTEND
DFMD19	EXTEND
DFMD23	EXTEND
DFMD24	EXTEND
DFMD26	EXTEND
DFMD27	EXTEND

CCI: CCI-000035

Group ID (Vulid): V-17985
Group Title: ZB000060
Rule ID: SV-32015r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTD0060
Rule Title: BMC CONTROL-D security exits are not installed or configured properly.

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

CTDSE01
CTDSE04
CTDSE08
CTDSE19
CTDSE24
CTDSE28

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

CTDSE01

CTDSE04
 CTDSE08
 CTDSE19
 CTDSE24
 CTDSE28

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-31828r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCTDR000
 Rule Title: BMC CONTROL-D installation data sets are not properly protected.

Vulnerability Discussion: BMC CONTROL-D 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:

A) Check with your IOA or Systems Programming personnel and compile the list of BMC CONTROL-D Installation Datasets. Most likely they are similar to SYS2.IOA.*.CTD*.*.

1. From the Administrator Main Menu Choose Option 2 Security Server Commands.
2. Choose Option 3 Data Set.
3. Type the resource names collected in option A) 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 specify UPDATE or READ.

8. Tab down to Standard Access Permits and place an E next to it and hit enter and
verify that UPDATE or higher access is limited to Systems Programming personnel. Verify Read access is given to:
 - Auditors
 - BMC Users
 - Security Personnel (Centralized)
 - Security Personnel (De-centralized)
 - BMC STCs
 - Batch Users.
 9. 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 Authorized Users if applicable.
 10. Repeat steps 2 through 10 for all datasets, if needed.
- B) If A.7, A.8, A.9 and A.10 are all true, there is NO FINDING.
- C) If A.7, A.8, A.9 and A.10 are not true, this is a FINDING.

Fix Text: The IAO will ensure that UPDATE and/or greater access to BMC CONTROL-D installation data sets are limited to System Programmers only, and all UPDATE and/or greater access is logged. READ access can be given to auditors, BMC users, security personnel (domain level and decentralized), and BMC STCs and/or batch users. All failures and successful UPDATE 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.*.CTDI.

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

```
ad 'SYS2.IOA.*.CTDI.**' uacc(none) owner(sys2) -
    audit(success(update) failures(read)) -
    data('BMC CONTROL-D Install DS')
pe 'SYS2.IOA.*.CTDI.**' id(<sypaudt>) acc(a)
pe 'SYS2.IOA.*.CTDI.**' id(<audtaudt> <secaudt> <secdaudt>) acc(r)
pe 'SYS2.IOA.*.CTDI.**' id(<bmcuser> CONTROL-D) acc(r)
```

setr generic(dataset) refresh

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-32166r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTDR001
Rule Title: BMC CONTROL-D STC data sets are not properly protected.

Vulnerability Discussion: BMC CONTROL-D 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:

A). Check with your IOA or Systems Programming personnel and compile the list of BMC Control-D STC and/or batch datasets. Most likely they are similar to:
SYS3.IOA.*.CTDO.**.

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

Commands

2. Choose Option 3 Data Set
3. Type the resource names collected in option A) 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 specify UPDATE or READ.
8. Tab down to Standard Access Permits and place an E next to it (hit enter).
 Validate that UPDATE or higher access is limited to Systems Programming personnel.
 Validate that UPDATE access is permitted to centralized and decentralized users.
 Validate that UPDATE or higher access is limited to BMC STCs and/or Batch Users.
 Verify READ access is permitted to Auditors and Control-D end-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 or higher access is limited to Systems Programming personnel. Validate that UPDATE access is permitted to centralized and decentralized users, BMC STCs and/or Batch users.
 Verify Read access is permitted to Auditors and Control-D end-users.
10. Repeat steps 1 through 9 for all datasets in option A) above.

B) If A.7, A.8, A.9 and A.10 are all true, there is NO FINDING.

C) If A.7, A.8, A.9 and A.10 are not true, this is a FINDING.

Fix Text: The IAO will ensure that UPDATE and/or greater access to BMC CONTROL-D

STC data sets are limited to System Programmers. ALTER access can be given to BMC STCs and/or batch users. UPDATE access can be given to centralized and decentralized security personnel. 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. 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.*.CTDO.

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

```
ad 'SYS3.IOA.*.CTDO.**' uacc(none) owner(sys3) -
    audit(failures(read)) -
    data('BMC CONTROL-D STC DS')
pe 'SYS3.IOA.*.CTDO.**' id(syspau dt tstcaudt) acc(a)
pe 'SYS3.IOA.*.CTDO.**' id(BMC STCs) acc(a)
pe 'SYS3.IOA.*.CTDO.**' id(secaaudt secdaudt) acc(u)
pe 'SYS3.IOA.*.CTDO.**' id(bmcuser audtaudt) acc(r)
```

setr generic(dataset) refresh

CCI: CCI-001499

Group ID (Vulid): V-21592
 Group Title: ZB000002
 Rule ID: SV-32163r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCTDR002
 Rule Title: BMC CONTROL-D User data sets are not properly protected.

Vulnerability Discussion: BMC CONTROL-D User data sets, CDAM and 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:

A) Check with your IOA or Systems Programming personnel and compile the list of

CONTROL-D user data sets. Most likely: they are similar to:

```
. SYS3.IOA.*.CTDR.**
CTRUSR.**
CTDSRV.**
CTDJB1.**
```

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

2. Choose Option 3 Data Set

3. Type the resource names collected in option A) 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 specify UPDATE or READ.

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

Validate Read access is limited to Auditors and any of the rest of the users

below.

Validate that UPDATE access is permitted to centralized and decentralized

security personnel, and CONTROL-D end users and any of the rest of the users

below.

Validate that UPDATE or higher access is permitted to Systems Programming

personnel AND BMC STCs AND Batch 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 Read access is limited to Auditors and any of the rest of the users

below.

Validate that UPDATE access is permitted to centralized and decentralized

security personnel, and CONTROL-D end users and any of the rest of the users

below.

Validate that UPDATE or higher access is permitted to Systems Programming

personnel AND BMC STCs AND Batch Users,

10.Repeat steps 1 through 9 for all datasets in option A) above.

B) If A.7, A.8, A.9 and A.10 are all true, there is NO FINDING.

C) If A.7, A.8, A.9 and A.10 are not true, this is a FINDING.

Fix Text: The IAO must ensure that UPDATE and/or greater access to BMC CONTROL-D

User data sets are limited to System Programmers and BMC STCs and/or batch

users. Additionally, UPDATE access can be given to centralized and decentralized security personnel, and BMC users. 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.*.CTDR.
CTRUSR.
CTDSRV.
CTDJB1.

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

```
ad 'SYS3.IOA.*.CTDR.**' uacc(none) owner(sys3) -
audit(failures(read)) -
data('BMC CONTROL-D Repository DS')
pe 'SYS3.IOA.*.CTDR.**' id(syspau dt tstcau dt BMC STCs) acc(a)
pe 'SYS3.IOA.*.CTDR.**' id(bmcuser) acc(u)
pe 'SYS3.IOA.*.CTDR.**' id(secau dt secdau dt) acc(u)
pe 'SYS3.IOA.*.CTDR.**' id(au dt au dt) acc(r)
```

```
ad 'CTRUSR.**' uacc(none) owner(CTRUSR) -
audit(failures(read)) -
data('BMC CONTROL-D CDAM DS')
pe 'CTRUSR.**' id(syspau dt tstcau dt BMC STCs) acc(a)
pe 'CTRUSR.**' id(bmcuser) acc(u)
pe 'CTRUSR.**' id(secau dt secdau dt) acc(u)
pe 'CTRUSR.**' id(au dt au dt) acc(r)
```

```
ad 'CTDSRV.**' uacc(none) owner(CTDSRV) -
audit(failures(read)) -
data('BMC CONTROL-D CDAM DS')
pe 'CTDSRV.**' id(syspau dt tstcau dt BMC STCs) acc(a)
pe 'CTDSRV.**' id(bmcuser) acc(u)
```

```

pe 'CTDSRV.**' id(secaaudt secdaudt) acc(u)
pe 'CTDSRV.**' id(audtaudt) acc(r)

ad 'CTDJB1.**' uacc(none) owner(CTDJB1) -
audit(failures(read)) -
data('BMC CONTROL-D CDAM DS')
pe 'CTDJB1.**' id(syspau dt tstcaudt BMC STCs) acc(a)
pe 'CTDJB1.**' id(bmcuser) acc(u)
pe 'CTDJB1.**' id(secaaudt secdaudt) acc(u)
pe 'CTDJB1.**' id(audtaudt) acc(r)

```

```
setr generic(dataset) refresh
```

CCI: CCI-001499

Group ID (Vulid): V-17947
 Group Title: ZB000020
 Rule ID: SV-32056r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCTDR020
 Rule Title: BMC CONTROL-D resources are not properly defined and protected.

Vulnerability Discussion: BMC CONTROL-D 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-D Resources table in the z/OS STIG Addendum are properly restricted.

Note: To determine what resource class is used review the IOACCLASS 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-D 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-D Resources table in the z/OS STIG

Addendum:

1. From the Administrator Main Menu Chose Option 3 Security Server Reports

2. Choose 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-D Resources table in the z/OS

STIG Addendum.

If TYPE is GROUP, place an S in the CMD line and hit enter to explode the GROUP.

7. 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-D 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-D Resources table in the z/OS STIG Addendum, then there is a FINDING.

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 IOAClass 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-D 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:

```
rdef $ioa $$addnot.** uacc(none) owner(admin)
    audit(failure(read)) -
    data('protected per zctdr020')

pe $$addnot.** cl($ioa) id(<appsaudt>) acc(alter)
pe $$addnot.** cl($ioa) id(<operaudt>) acc(alter)
pe $$addnot.** cl($ioa) id(<pcspaudt>) acc(alter)
pe $$addnot.** cl($ioa) id(<sypaudt>) acc(alter)
```

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17452
 Group Title: ZB000030
 Rule ID: SV-32068r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCTDR030
 Rule Title: BMC CONTROL-D Started Task name is not properly identified / defined to the system ACP.

Vulnerability Discussion: Products that require a started task will require that the started task 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 CONTROLD; Press ENTER
- d) If not found then CONTROLD; 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-D started task is defined to the security database and is protected, there is NO FINDING.
- j) If the userid for the CONTROL-D 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 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 CONTROLD name('stc, BMC ControlD') owner(stc) dfltgrp(stc) nopass
```

CCI: CCI-000764

Group ID (Vulid): V-17454
 Group Title: ZB000032
 Rule ID: SV-32155r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCTDR032
 Rule Title: BMC CONTROL-D 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:

a) Use Vanguard's Analyzer product to look at the Started Procedures Analysis report:

1. From Analyzer main Menu, go to 3;4; Press ENTER
2. Key in SORT PROCNAME; Press ENTER
3. Key in L CONTROLD or the name of the CONTROLD 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 CONTROLD started task is not defined to RACF as a STC user.

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

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

Fix Text: The BMC CONTROL-D 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 CONTROLD started task thru a corresponding STARTED class entry.

A sample set of commands is shown here:

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

CCI: CCI-000764

UNCLASSIFIED