VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

z/OS BMC CONTROL-D for TSS STIG

Version: 6

Release: 7

26 Oct 2018

XSL Release 1/29/2015 Sort by: STIGID

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.

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(ZCTD0040)

The following keywords will have the specified values 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

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.

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-31830r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTDT000
Rule Title: BMC CONTROL-D installation data sets will be 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.

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

- SENSITVE.RPT(CTDRPT)

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

- PDI(ZCTD0000)

Verify that the accesses to the BMC CONTROL-D 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, BMC users, security 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-D
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, BMC
users, security 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.*.CTDI.

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

```
TSS PERMIT(<syspaudt>) DSN(SYS2.IOA.*.CTDI.) ACCESS(R)
TSS PERMIT(<syspaudt>) DSN(SYS2.IOA.*.CTDI.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<audtaudt>) DSN(SYS2.IOA.*.CTDI.) ACCESS(R)
TSS PERMIT(<bmcuser>) DSN(SYS2.IOA.*.CTDI.) ACCESS(R)
TSS PERMIT(<secaaudt>) DSN(SYS2.IOA.*.CTDI.) ACCESS(R)
TSS PERMIT(<secdaudt>) DSN(SYS2.IOA.*.CTDI.) ACCESS(R)
TSS PERMIT(<CONTROLD>) DSN(SYS2.IOA.*.CTDI.) ACCESS(R)
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-32167r3_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTDT001
Rule Title: BMC CONTROL-D STC data sets must be 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.

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

- SENSITVE.RPT(CTDSTC)

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

- PDI(ZCTD0001)

Verify that the accesses to the BMC CONTROL-D STC 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 and CONTROL-D end users.

___ 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 BMC STCs and/or batch users.

___ The TSS data set access authorizations restrict UPDATE access to
centralized and decentralized security personnel.

Fix Text: The IAO will ensure that WRITE and/or greater access to BMC CONTROL-D
STC data sets are limited to System Programmers and 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:

```
TSS PERMIT(syspaudt) DSN(SYS3.IOA.*.CTDO.) ACCESS(ALL)
```

```
TSS PERMIT(tstcaudt) DSN(SYS3.IOA.*.CTDO.) ACCESS(ALL)
TSS PERMIT(BMC STCs) DSN(SYS3.IOA.*.CTDO.) ACCESS(ALL)
TSS PERMIT(secaaudt) DSN(SYS3.IOA.*.CTDO.) ACCESS(U)
TSS PERMIT(secdaudt) DSN(SYS3.IOA.*.CTDO.) ACCESS(U)
TSS PERMIT(audtaudt) DSN(SYS3.IOA.*.CTDO.) ACCESS(R)
TSS PERMIT(bmcuser) DSN(SYS3.IOA.*.CTDO.) ACCESS(R)

CCI: CCI-001499
```

```
 Group ID (Vulid):  V-21592
Group Title:  ZB000002
Rule ID:  SV-32164r3_rule
Severity: CAT II
 Rule Version (STIG-ID):  ZCTDT002
Rule Title: BMC CONTROL-D user data sets must be 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.


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(ZCTD0002)

Verify that the accesses to the BMC CONTROL-D 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 CONTROL-D's STC(s) and/or batch user(s).
```

___ The TSS data set access authorizations restrict UPDATE access to centralized
and decentralized security personnel, and/or CONTROL-D end users.

Fix Text: The IAO must ensure that WRITE 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:

```
TSS PERMIT(syspaudt) DSN(SYS3.IOA.*.CTDR.) ACCESS(ALL)
TSS PERMIT(tstcaudt) DSN(SYS3.IOA.*.CTDR.) ACCESS(ALL)
TSS PERMIT(BMC STCs) DSN(SYS3.IOA.*.CTDR.) ACCESS(ALL)
TSS PERMIT(bmcuser) DSN(SYS3.IOA.*.CTDR.) ACCESS(U)
TSS PERMIT(secaaudt) DSN(SYS3.IOA.*.CTDR.) ACCESS(U)
TSS PERMIT(secdaudt) DSN(SYS3.IOA.*.CTDR.) ACCESS(U)
TSS PERMIT(audtaudt) DSN(SYS3.IOA.*.CTDR.) ACCESS(R)

TSS PERMIT(syspaudt) DSN(CTRUSR.) ACCESS(ALL)
TSS PERMIT(tstcaudt) DSN(CTRUSR.) ACCESS(ALL)
TSS PERMIT(BMC STCs) DSN(CTRUSR.) ACCESS(ALL)
TSS PERMIT(bmcuser) DSN(CTRUSR.) ACCESS(U)
```

```
TSS PERMIT(secaaudt) DSN(CTRUSR.) ACCESS(U)
TSS PERMIT(secdaudt) DSN(CTRUSR.) ACCESS(U)
TSS PERMIT(audtaudt) DSN(CTRUSR.) ACCESS(R)

TSS PERMIT(syspaudt) DSN(CTDSRV.) ACCESS(ALL)
TSS PERMIT(tstcaudt) DSN(CTDSRV.) ACCESS(ALL)
TSS PERMIT(BMC STCs) DSN(CTDSRV.) ACCESS(ALL)
TSS PERMIT(bmcuser) DSN(CTDSRV.) ACCESS(U)
TSS PERMIT(secaaudt) DSN(CTDSRV.) ACCESS(U)
TSS PERMIT(secdaudt) DSN(CTDSRV.) ACCESS(U)
TSS PERMIT(audtaudt) DSN(CTDSRV.) ACCESS(R)

TSS PERMIT(syspaudt) DSN(CTDJB1.) ACCESS(ALL)
TSS PERMIT(tstcaudt) DSN(CTDJB1.) ACCESS(ALL)
TSS PERMIT(BMC STCs) DSN(CTDJB1.) ACCESS(ALL)
TSS PERMIT(bmcuser) DSN(CTDJB1.) ACCESS(U)
TSS PERMIT(secaaudt) DSN(CTDJB1.) ACCESS(U)
TSS PERMIT(secdaudt) DSN(CTDJB1.) ACCESS(U)
TSS PERMIT(audtaudt) DSN(CTDJB1.) ACCESS(R)

CCI: CCI-000213
```

```
 Group ID (Vulid):  V-17947
Group Title:  ZB000020
Rule ID:  SV-32057r3_rule
Severity: CAT II
 Rule Version (STIG-ID):  ZCTDT020
Rule Title: BMC CONTROL-D resources must be 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.


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

- SENSITVE.RPT(ZCTD0020)

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

- PDI(ZCTD0020)

Verify that the accesses to resources and/or generic equivalent are properly
restricted according to the requirements specified in BMC CONTROL-D 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: 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. 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-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:

```
TSS ADD(ADMIN) IOA($$ADDNOT)
TSS PERMIT(<appsaudt>) IOA($$ADDNOT) ACC(ALL)
TSS PERMIT(<operaudt>) IOA($$ADDNOT) ACC(ALL)
TSS PERMIT(<pcspaudt>) IOA($$ADDNOT) ACC(ALL)
TSS PERMIT(<syspaudt>) IOA($$ADDNOT) ACC(ALL)
```

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-32069r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTDT030
Rule Title: BMC CONTROL-D Started Task name is not properly identified / defined
to the system ACP.

Vulnerability Discussion: BMC CONTROL-D 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-D STC/Batch ACID(s) for the following:

___ Defined with Facility of STC and/or BATCH.

___ Defined with Master Facility of CONTROLD.

___ Is sourced to the INTRDR.

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.

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(CONTROLD) TYPE(USER) -
       NAME('*STC* for CONTROL-D') DEPT(xxxx) -
      FAC(STC) -
      MASTFAC(CONTROLD) PASS(xxxxxxxx,0) -
      SOURCE(INTRDR) NOSUSPEND
```

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-32156r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTDT032
Rule Title: BMC CONTROL-D 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(ZCTD0032)

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

Fix Text: The BMC CONTROL-D 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-D 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(CONTOLD) ACID(CONTROLD)

CCI: CCI-000764

Group ID (Vulid): V-17469
Group Title: ZB000036
Rule ID: SV-32053r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTDT036
Rule Title: BMC CONTROL-D is not properly defined to the Facility Matrix Table
for Top Secret.

Vulnerability Discussion: Improperly defined security controls for the BMC
CONTROL-D 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-D Facility Matrix table is defined as follows:

FAC(USERxx=NAME=CONTROLD,PGM=CTD,ID=nn,ACTIVE,SHRPRF)
FAC(CONTROLD=ASUBM,NOABEND,MULTIUSER,NOXDEF,SIGN(S))
FAC(CONTROLD=RES,LUMSG,STMSG,WARNPW,NORNDPW)
FAC(CONTROLD=NOAUDIT,NOTSOC,MODE=FAIL)

FAC(CONTROLD=LOG(SMF,INIT,MSG,SEC9),UIDACID=8,LOCKTIME=000)

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

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

CCI: CCI-000764
