VANGUARD
INTEGRITY PROFESSIONALS
INFORMATION SECURITY EXPERTS

z/OS BMC MAINVIEW for z/OS for RACF STIG

Version: 6

Release: 8

31 Oct 2017

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

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-33836r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZMVZR000
Rule Title: BMC MAINVIEW for z/OS installation data sets are not properly protected.

Vulnerability Discussion: BMC MAINVIEW for z/OS 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 MAINVIEW for z/OS Installation Datasets, Likely:
1.   SYS2.BMCVIEW.**
 SYS3.BMCVIEW.**
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)and validate that UPDATE or higher access is limited to Systems
Programming personnel. All Authorized Users (ID(*)) are allowed READ
(any user
may be permitted read).
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. All Authorized Users (ID(*)) are allowed READ.
11.   Repeat steps 2 through 10 for all datasets in option a.1

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 alter access to BMC
MAINVIEW for
z/OS 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.BMCVIEW.**
SYS3.BMCVIEW.** (data sets that are not altered by product STCs, can be more specific)

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

```
ad 'SYS2.BMCVIEW.**' uacc(none) owner(sys2) -
       audit(success(update) failures(read)) -
      data('BMC MAINVIEW for z/OS Install DS')
pe 'SYS2.BMCVIEW.**' id(<syspaudt> <tstcaudt>) acc(a)
pe 'SYS2.BMCVIEW.**' id(<audtaudt> authorized users) acc(r)
pe 'SYS2.BMCVIEW.**' id(MAINVIEW STCs)

ad 'SYS3.BMCVIEW.**' uacc(none) owner(sys3) -
       audit(success(update) failures(read)) -
      data('BMC MAINVIEW for z/OS Install DS')
pe 'SYS3.BMCVIEW.**' id(<syspaudt> <tstcaudt>) acc(a)
pe 'SYS3.BMCVIEW.**' id(<audtaudt> authorized users) acc(r)
pe 'SYS3.BMCVIEW.**' id(MAINVIEW STCs)

setr generic(dataset) refresh
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-37723r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZMVZR001
Rule Title: BMC MAINVIEW for z/OS STC data sets are not properly protected.

Vulnerability Discussion: BMC MAINVIEW for z/OS 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 MAINVIEW STC datasets, Likely:
1.   hlq.BMCVIEW.**
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.   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, BMC Mainview STCs and/or BMC Batch Jobs. Read
access can
be permitted to Auditors and all authorized 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.
READ
access can be permitted to Auditors and all authorized users.

10.   Repeat steps 2 through 9 for all datasets in option a.1

b) If a.7, a.8, and a.9 are all true, there is NO FINDING.

c) If a.7, a.8, and a.9 are not true, this is a FINDING.

Fix Text: The IAO will ensure that update and allocate access to BMC
MAINVIEW
for z/OS STC data sets is limited to System Programmers and/or BMC
MAINVIEW for
z/OS s STC(s) and/or batch user(s) only. Read access can be given to
auditors
and 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 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.BMCVIEW (data sets that are altered by the product s STCs, this can be more specific)

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

```
ad 'SYS3.BMCVIEW.**' uacc(none) owner(sys3) -
       audit(failures(read)) -
      data('Vendor DS Profile: BMC MAINVIEW for z/OS')
pe 'SYS3.BMCVIEW.**' id(<syspaudt> <tstcaudt> MAINVIEW STCs) acc(a)
pe 'SYS3.BMCVIEW.**' id(<audtaudt> authorized users) acc(r)

setr generic(dataset) refresh
```

CCI: CCI-001499

Group ID (Vulid): V-17947

Group Title: ZB000020

Rule ID: SV-46312r2_rule

Severity: CAT II

Rule Version (STIG-ID): ZMVZR020

Rule Title: BMC MAINVIEW resources must be properly defined and protected.

Vulnerability Discussion: BMC MAINVIEW 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:
a) From the Administrator main menu, select 3;4 (Security Server Reports, General Resource Profiles) and press ENTER.

b) Tab down to CLASS , type #BMCVIEW or whatever class has been set up for BMC Mainview Resources (find out from your IOA)on your system and press ENTER.

1. Look for the profiles in the Profile Name column that are listed in the BMC Mainview resource table, resource column in the z/OS STIG Addendum.
2. Ensure that they are defined with a UACC=NONE in the UACC column.
3. If all UACCs are NONE, there is NO FINDING on this point.
4. If any UACC is not equal to NONE, this is a FINDING.

c) Type LR in the CMD column of each resource name listed in the table below and check that.

1. Warning = NO.
2. The access list showing list of users, only includes valid users per the resources table.
3. The users only have the level of access permitted per the BMC Mainview resource table.

** (To check if a user belongs to one of the groups in the BMC MAINVIEW RESOURCES table:

- Select Option 3;2 from the Administrator Main Menu (Security Server Reports, Group Profiles)
- On the Group Reports Menu, enter 1 at the Command line (for Group Profile Summary)
- Then tab down to Group and enter the Group Name from the resources table and hit enter.
- On the next panel enter LV next to the group name and hit enter
- The General Information Screen that comes up will have the list of Connected Users.

d) If

- WARNING is not set to NO or
- any users or groups are granted access who are not in the BMC MAINVIEW Resource Table
- or any users or groups are granted access that is not permitted to them per the BMC MAINVIEW resource table there is a FINDING.

e) If none of the conditions in d. above are true then there is NO FINDING.

Fix Text: The IAO will work with the systems programmer to verify that the following are properly specified in the ACP.

(Note: The resource class, resources, and/or resource prefixes identified below are examples of a possible installation. The actual resource class, resources, 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.)

Use BMC MAINVIEW Resources table in the zOS STIG Addendum. This table lists the resources, access requirements, and logging requirement for BMC MAINVIEW. Ensure the guidelines for the resources and/or generic equivalent specified in the z/OS STIG Addendum are followed.

The RACF resources as designated in the above table are defined with a default access of NONE.

The RACF resource access authorizations restrict access to the appropriate personnel as designated in the above table.

The RACF resource rules for the resources designated in the above table specify UACC(NONE) and NOWARNING.

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

```
RDEFINE #BMCVIEW BBM.ssid.CN UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
PERMIT BBM.ssid.CN CLASS(#BMCVIEW) ACCESS(ALTER) ID(autoaudt)
PERMIT BBM.ssid.CN CLASS(#BMCVIEW) ACCESS(ALTER) ID(dasdaudt)
PERMIT BBM.ssid.CN CLASS(#BMCVIEW) ACCESS(ALTER) ID(mqsaaudt)
PERMIT BBM.ssid.CN CLASS(#BMCVIEW) ACCESS(ALTER) ID(Mainview STCs)
PERMIT BBM.ssid.CN CLASS(#BMCVIEW) ACCESS(ALTER) ID(mvzread)
PERMIT BBM.ssid.CN CLASS(#BMCVIEW) ACCESS(ALTER) ID(mvzupdt)
PERMIT BBM.ssid.CN CLASS(#BMCVIEW) ACCESS(ALTER) ID(pcspaudt)
PERMIT BBM.ssid.CN CLASS(#BMCVIEW) ACCESS(ALTER) ID(syspaudt)
```

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-33839r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZMVZR030

Rule Title: BMC Mainview for z/OS Started Task name is not properly identified and/or defined to the system ACP.

Vulnerability Discussion: BMC Mainview for z/OS 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) Use Vanguards Analyzer product to look at the Started Procedures Analysis report: Do the following for the BMC MAINVIEW started task, likely called MV$CAS or MV$PAS or MV$MVS.

a. From Analyzer main Menu, go to 3;4; Press ENTER
b. Key in SORT PROCNAME; Press ENTER
c. Key in L MV$; Press ENTER
d. If the STC name is not found then BMC MAINVIEW is not defined to RACF as a STC user.
e. If STC name is found but has an R in the M column, review the message and ensure that the following does not appear: VSA346R The user ID does not have the protected attribute. If message exists, then user does not have the PROTECTED attribute. This is a finding.
f. If found then you would use the U line command to determine if the userid is defined to RACF.
g. Key the U line command for the BMC MAINVIEW entry; Press ENTER
h. The userid is defined to RACF if a userid display appears. If not defined you should see the message No data to display.

b) If the userid for the BMC MAINVIEW started task is defined to the security database with the PROTECTED attribute, there is NO FINDING.

c) If the userid for the BMC MAINVIEW started task is not defined to the security database or does not have the PROTECTED attribute, this is a FINDING

Fix Text: The BMC Mainview for z/OS system programmer and the IAO will ensure that a product's Started Task(s) is properly identified and/or 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 MV$CAS name('CAS, BMC Mainview for z/OS') owner(stc) dfltgrp(stc)
nopass
au MV$PAS name('PAS, BMC Mainview for z/OS') owner(stc) dfltgrp(stc)
nopass
au MV$MVS name('MVS, BMC Mainview for z/OS') owner(stc) dfltgrp(stc)
nopass
```

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-33841r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZMVZR032
Rule Title: BMC Mainview for z/OS Started task(s) must be 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 Vanguards Analyzer product to look at the Started Procedures Analysis report: Look for the name of the BMC Mainview started task. The name is

likely MV$CAS and/or MV$PAS and/or MV$MVS
1. From Analyzer main Menu, go to 3;4; Press ENTER
2. Key in SORT PROCNAME; Press ENTER
3. Key in L MV$ or your site's name for the BMC Mainview started task;
Press ENTER
4. Look at the source column. It will indicate STARTED class profile or
ICHRIN03 entry.
5. If not found then BMC Mainview STC is not defined to RACF as an STC
user.

b) If a STARTED resource class profile exists for the BMC Mainview started
task, there is NO FINDING.

c) If neither a STARTED resource class profile or an ICHRIN03 entry exists
for the for BMC Mainview started task, this is a FINDING.

Fix Text: The BMC Mainview 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 userid must be assigned for the BMC Mainview started task(s) thru a
corresponding STARTED class entry.

The following sample set of commands is shown here as a guideline:

```
rdef started MV$CAS.** uacc(none) owner(admin) audit(all(read))
stdata(user(MV$CAS) group(stc))
rdef started MV$MVS.** uacc(none) owner(admin) audit(all(read))
stdata(user(MV$MVS) group(stc))

setr racl(started) ref
```

CCI: CCI-000764

Group ID (Vulid): V-18011
Group Title: ZB000038
Rule ID: SV-33845r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZMVZR038
Rule Title: BMC Mainview for z/OS Resource Class will be defined or active in
the ACP.

Vulnerability Discussion: Failure to use a robust ACP to control a product could potentially compromise the integrity and availability of the MVS operating system and user data.

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

Check Content:
a) Determine which class is being used for MAINVIEW RACF Security.

b) Use Vanguards Administrator product validate that the CLASS is active.

1. From Administrator main menu, select option 2. Security Server Commands.

2. Select SETROPTS option 5 SETROPTS option,

3. On the SETROPTs screen, locate the CDT Classes prompt, enter E next to it.

4. Invoke the locate command, Locate class found in step a.

c) Screen print the display showing the attributes of the class, including active status
1. If the class is ACTIVE there is NO FINDING
2. If the class is not ACTIVE there is a FINDING

Fix Text: The IAO will ensure that the BMC Mainview for z/OS Resource Class(es) is (are) active.

Use the following commands as an example:

```
RDEFINE CDT class -
CDTINFO( MAXLENGTH(64) DEFAULTUACC(NONE) -
FIRST(ALPHA) CASE(UPPER) -
OTHER(ALPHA,NUMERIC,NATIONAL,SPECIAL) -
POSIT(301) RACLIST(REQUIRED) -
GENERIC(ALLOWED) GENLIST(ALLOWED) -
OPERATIONS(YES) -
) UACC(NONE)

SETROPTS CLASSACT(CDT) RACLIST(CDT)
SETROPTS RACLIST(CDT) REFRESH

SETROPTS GENERIC(class) GENCMD(class)
SETROPTS CLASSACT(class) RACLIST(class)
SETROPTS RACLIST(class) REFRESH
```

CCI: CCI-000336

CCI: CCI-002358

Group ID (Vulid): V-18014
Group Title: ZB000040
Rule ID: SV-37807r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZMVZR040
Rule Title: BMC MAINVIEW for z/OS configuration/parameter values are not specified properly.

Vulnerability Discussion: BMC MAINVIEW for z/OS configuration/parameters controls 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 steps are necessary for reviewing the BMC MAINVIEW options:

a) Have the products system programmer display the configuration/parameters control statements used in the current running product to define or enable security Refer to the Configuration Location dataset and member specified in the z/OS Dialog Management Procedures for BMC MAINVIEW for z/OS. Verify the following specifications:

Keyword	Value
ESMTYPE	(AUTO|RACF)

b) If (a) above is true, there is NO FINDING.

c) If (a) above is untrue, this is a FINDING

Fix Text: The BMC MAINVIEW for z/OS 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 MAINVIEW for z/OS security parameters for the specific
ACP
environment along with additional IOA security parameters with standard
values
as documented below.

Statement(values)
ESMTYPE(AUTO|RACF)

CCI: CCI-000035
____

UNCLASSIFIED