

VANGUARD

Integrity Professionals, Inc.

Enterprise Security Software

z/OS BMC MAINVIEW for z/OS for ACF2 STIG

Version: 6

Release: 8

29 Dec 2020

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:

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

- SENSITVE.RPT(MVZRPT)

Automated Analysis

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

- PDI(ZMVZ0000)

Verify that the accesses to the BMC MAINVIEW for z/OS installation data sets are properly restricted.

___ The ACF2 data set rules for the data sets restricts READ access to all authorized users.

___ The ACF2 data set rules for the data sets restricts UPDATE and/or ALTER access to systems programming personnel.

___ The ACF2 data set rules for the data sets specify that all (i.e., failures and successes) UPDATE and/or ALTER access are logged

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:

```
$KEY(SYS3)
BMCVIEW.- UID(<syspautd>) R(A) W(A) A(A) E(A)
BMCVIEW.- UID(<tstcaudt>) R(A) W(A) A(A) E(A)
BMCVIEW.- UID(MAINVIEW STCs) R(A) W(A) A(A) E(A)
BMCVIEW.- UID(<audtaudt>) R(A) E(A)
BMCVIEW.- UID(authorize users) R(A) E(A)
```

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:

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

- SENSITVE.RPT(MVZSTC)

Automated Analysis

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

- PDI(ZMVZ0001)

Verify that the accesses to the BMC MAINVIEW for z/OS STC data sets are properly restricted.

____ The ACF2 data set rules for the data sets restricts READ access to auditors and authorized users.

____ The ACF2 data set rules for the data sets restricts UPDATE and/or ALTER access to systems programming personnel.

____ The ACF2 data set rules for the data sets restricts UPDATE and/or ALTER access to the BMC MAINVIEW for z/OS s STC(s) and/or batch user(s).

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(<syspautd> <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:
Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITVE.RPT(ZMVZ0020)

- ACF2CMDS.RPT(RESOURCE) Alternate report

Automated Analysis

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

- PDI(ZMVZ0020)

Verify that the accesses to resources and/or generic equivalent are properly restricted according to the requirements specified in BMC MAINVIEW Resources table in the z/OS STIG Addendum. If the following guidance is true, this is not a finding.

___ The ACF2 resources are defined with a default access of PREVENT.

___ The ACF2 resource access authorizations restrict access to the appropriate personnel.

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

(Note: The resource type, resources, and/or resource prefixes identified below are examples of a possible installation. The actual resource type, 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 z/OS STIG Addendum. This table lists the resources, access requirements, and logging requirement for BMC MAINVIEW. Ensure the guidelines for the resource type, resources, and/or generic equivalent specified in the z/OS STIG Addendum are followed.

The ACF2 resources as designated in the above table are defined with a default access of PREVENT.

The ACF2 resource access authorizations restrict access to the appropriate personnel as designated in the above table.

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

```
$KEY(BBM) TYPE(BMV)
ssid.CN UID(autoaudt) ALLOW
ssid.CN UID(dasdaudt) ALLOW
ssid.CN UID(mqsaaudt) ALLOW
ssid.CN UID(Mainview STCs) ALLOW
ssid.CN UID(mvzread) ALLOW
ssid.CN UID(mvzupdt) ALLOW
ssid.CN UID(pcsaudt) ALLOW
ssid.CN UID(syspaudt) ALLOW
- UID(*) PREVENT
```

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:

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

- ACF2CMDS.RPT(ATTSTC)

Insure that the logonids(s) for the BMC Mainview for z/OS started task(s) includes the following:

STC

NO-SMC

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-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

IACControls: DCCS-1, DCCS-2

Check Content:

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

- ACF2CMDS.RPT(ACFGSO)

Ensure that the following GSO CLASMAP record entries are defined:

CLASMAP.class RESOURCE(class) RSRCTYPE(type) ENTITYLN(39)

Ensure that the following GSO SAFDEF record entries are defined:

INSERT SAFDEF.ssid ID(BBCS) MODE(GLOBAL)REP -
RACROUTE(SUBSYS=ssid REQSTOR=-)

Fix Text: The IAO will use SAF security to define and protect the Products resource class(es).

Ensure that the following GSO CLASMAP record entry(ies) is (are) defined:

CLASMAP.class RESOURCE(class) RSRCTYPE(type) ENTITYLN(39)

Example:

```
SET C(GSO)
LIST CLASMAP.BMCVIEW
INSERT CLASMAP.BMCVIEW ENTITYLN(39) RESOURCE(BMCVIEW) RSRCTYPE(BBM)
```

F ACF2,REFRESH(CLASMAP)

Ensure that the following GSO SAFDEF record entry(ies) is (are) defined:

SAFDEF.ssid ID(BBCS) MODE(GLOBAL)REP RACROUTE(SUBSYS=ssid REQSTOR=-)

Example:

```
ACF
SET C(GSO)
LIST SAFDEF.ssid
INSERT SAFDEF.ssid ID(BBCS) MODE(GLOBAL)REP RACROUTE(SUBSYS=ssid REQSTOR=-)
```

F ACF2,REFRESH(SAFDEF)

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:
Refer to the Configuration Location dataset and member specified in the z/OS Dialog Management Procedures for BMC MAINVIEW for z/OS.

Automated Analysis
Refer to the following report produced by the z/OS Data Collection:

- PDI(ZMVZ0040)

The following keywords will have the specified values in the BMC MAINVIEW for z/OS security parameter member:

Statement(values)
ESMTYPE(AUTO|ACF2)

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