VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

z/OS BMC MAINVIEW for z/OS for TSS STIG
Version: 6
Release: 7
20 Jan 2015

XSL Release 1/29/2015 Sort by: STIGID

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-33837r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZMVZT000
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.

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 TSS data set rules for the data sets restricts READ access to all authorized users.

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

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

Fix Text: The IAO will ensure that update and allocate access to BMC MAINVIEW for z/OS 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 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:
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:

TSS PERMIT(<syspaudt>) DSN(SYS2.BMCVIEW.) ACCESS(R)
TSS PERMIT(<syspaudt>) DSN(SYS2.BMCVIEW.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<tstcaudt>) DSN(SYS2.BMCVIEW.) ACCESS(R)
TSS PERMIT(<tstcaudt>) DSN(SYS2.BMCVIEW.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<audtaudt>) DSN(SYS2.BMCVIEW.) ACCESS(R)
TSS PERMIT(authorized users) DSN(SYS2.BMCVIEW.) ACCESS(R)
TSS PERMIT(MAINVIEW STCs) DSN(SYS2.BMCVIEW.) ACCESS(R)
TSS PERMIT(<syspaudt>) DSN(SYS3.BMCVIEW.) ACCESS(R)
TSS PERMIT(<syspaudt>) DSN(SYS3.BMCVIEW.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<tstcaudt>) DSN(SYS3.BMCVIEW.) ACCESS(R)
TSS PERMIT(<tstcaudt>) DSN(SYS3.BMCVIEW.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<audtaudt>) DSN(SYS3.BMCVIEW.) ACCESS(R)
TSS PERMIT(authorized users) DSN(SYS3.BMCVIEW.) ACCESS(R)
TSS PERMIT(MAINVIEW STCs) DSN(SYS3.BMCVIEW.) ACCESS(R)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-37724r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZMVZT001
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.

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 TSS data set rules for the data sets restricts READ access to auditors and authorized users.

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

___ The TSS data set rules for the data sets restricts UPDATE and/or ALL 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:

TSS PERMIT(<syspaudt>) DSN(SYS3.BMCVIEW) ACCESS(ALL)
TSS PERMIT(<tstcaudt>) DSN(SYS3.BMCVIEW) ACCESS(ALL)

TSS PERMIT(MAINVIEW STCs) DSN(SYS3.BMCVIEW) ACCESS(ALL)
TSS PERMIT(<audtaudt>) DSN(SYS3.BMCVIEW) ACCESS(R)
TSS PERMIT(authorize user) DSN(SYS3.BMCVIEW) ACCESS(R)

CCI: CCI-001499

Group ID (Vulid): V-17947
Group Title: ZB000020
Rule ID: SV-46313r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZMVZT020
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.

IAControls: ECCD-1, ECCD-2

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

- SENSITVE.RPT(ZMVZ0020)
- TSSCMDS.RPT(#RDT)

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 TSS resources are owned or DEFPROT is specified for the resource class.

___ The TSS 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 class, resources, and/or resource prefixes identified below are examples of a possible installation. The resource class, actual 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 TSS resources as designated in the above table are owned and/or DEFPROT is specified for the resource class.

The TSS 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:

TSS ADD(dept-acid) #BMCVIEW(BBM)
TSS PERMIT(autoaudt) #BMCVIEW(BBM.ssid.CN) ACCESS(ALL)
TSS PERMIT(dasdaudt) #BMCVIEW(BBM.ssid.CN) ACCESS(ALL)
TSS PERMIT(mqsaaudt) #BMCVIEW(BBM.ssid.CN) ACCESS(ALL)
TSS PERMIT(Mainview STCs) #BMCVIEW(BBM.ssid.CN) ACCESS(ALL)
TSS PERMIT(mvzread) #BMCVIEW(BBM.ssid.CN) ACCESS(ALL)
TSS PERMIT(mvzupdt) #BMCVIEW(BBM.ssid.CN) ACCESS(ALL)
TSS PERMIT(pcspaudt) #BMCVIEW(BBM.ssid.CN) ACCESS(ALL)
TSS PERMIT(syspaudt) #BMCVIEW(BBM.ssid.CN) ACCESS(ALL)

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-33840r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZMVZT030
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.

IAControls: ECCD-1, ECCD-2

Check Content:
Refer to the following report produced by the TSS Data Collection:

- TSSCMDS.RPT(@ACIDS)

Review each BMC Mainview for z/OS STC/Batch ACID(s) for the following:

___ Defined with Facility of STC, BBI3 (the TSS FACILITY Matrix Table entry defined for this product), and/or BATCH for MV$CAS, MV$PAS, and MV$MVS.

___ Defined with Master Facility of BBI3 (the TSS FACILITY Matrix Table entry defined for this product) for MV$CAS and MV$PAS.

___ Is sourced to the INTRDR.

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:

```
TSS CREATE(MV$CAS) TYPE(USER) -
     NAME('CAS, BMC Mainview for z/OS') DEPT(xxxx) -
    FAC(STC,BBI3) -
    MASTFAC(BBI3) PASS(xxxxxxxx,0) -
    SOURCE(INTRDR) NOSUSPEND
TSS CREATE(MV$PAS) TYPE(USER) -
     NAME('PAS, BMC Mainview for z/OS') DEPT(xxxx) -
    FAC(STC,BBI3) -
    MASTFAC(BBI3) PASS(xxxxxxxx,0) -
    SOURCE(INTRDR) NOSUSPEND
TSS CREATE(MV$MVS) TYPE(USER) -
     NAME('MVS, BMC Mainview for z/OS') DEPT(xxxx) -
```

FAC(STC,BBI3) -
PASS(xxxxxxxx,0) -
SOURCE(INTRDR) NOSUSPEND

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-33842r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZMVZT032
Rule Title: BMC Mainview for z/OS 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.

IAControls: ECCD-1, ECCD-2

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(ZMVZ0032)

Verify that the BMC Mainview for z/OS started task(s) is (are) defined in the TSS STC record.

Fix Text: The BMC Mainview for z/OS 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 Mainview for z/OS 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(MV$CAS) ACID(MV$CAS)
TSS ADD(STC) PROCNAME(MV$MVS) ACID(MV$MVS)

CCI: CCI-000764

Group ID (Vulid): V-17469
Group Title: ZB000036
Rule ID: SV-33843r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZMVZT036
Rule Title: BMC Mainview for z/OS is not properly defined to the Facility Matrix Table for Top Secret.

Vulnerability Discussion: Improperly defined security controls for BMC Mainview for z/OS could result in the compromise of the network, operating system, and customer data.

IAControls: ECCD-1, ECCD-2

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 Mainview for z/OS Facility Matrix table is defined as follows:

BBI3:
FAC(USERxx=NAME=BBI3,PGM=BBM,ID=nn,ACTIVE,SHRPRF,ASUBM)
FAC(BBI3=NOABEND,MULTIUSER,NOXDEF,SIGN(S),RES,LUMSG)
FAC(BBI3=STMSG,WARNPW,NORNDPW,NOAUDIT,NOTSOC,MODE=FAIL)
FAC(BBI3=LOG(SMF,INIT,MSG,SEC9),UIDACID=8,LOCKTIME=000)

Fix Text: The BMC Mainview for z/OS system programmer and the IAO will ensure that the TOP SECRET Facility Matrix Table is proper defined using the following example:

**** BBI3
*
FACILITY(USERxx=NAME=BBI3,PGM=BBM,ID=nn,ACTIVE,SHRPRF)
FACILITY(BBI3=ASUBM,NOABEND,MULTIUSER,NOXDEF)
FACILITY(BBI3=LUMSG,STMSG,SIGN(S),NORNDPW)
FACILITY(BBI3=NOAUDIT,RES,WARNPW,NOTSOC)
FACILITY(BBI3=MODE=FAIL,LOG(SMF,INIT,MSG,SEC9))
FACILITY(BBI3=UIDACID=8,LOCKTIME=000)

CCI: CCI-000764

Group ID (Vulid): V-18011
Group Title: ZB000038
Rule ID: SV-33846r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZMVZT038
Rule Title: BMC Mainview for z/OS Resource Class must 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.

IAControls: DCCS-1, DCCS-2

Check Content:
Refer to the following report produced by the ACP Data Collection:

- TSSCMDS.RPT(#RDT)

If the BMC Mainview for z/OS Resource Class(es) is (are) defined in the Resource Definition Table (RDT) as follows, this is not a finding.

```
RESOURCE CLASS = class
RESOURCE CODE = X'hex code'
ATTRIBUTE = MASK|NOMASK,MAXOWN(08),MAXPERMIT(044),ACCESS,DEFPROT
ACCESS = NONE(0000),CONTROL(0400),UPDATE(6000),READ(4000)
ACCESS = WRITE(2000),ALL(FFFF)
DEFACC = READ
```

Fix Text: The IAO will ensure the BMC Mainview for z/OS resource class(es) is (are) defined in the TSS RDT.

(Note: The RESCLASS and/or RESCODE identified below are examples of a possible installation. The actual RESCLASS and/or RESCODE values are determined when the product is actually installed on a system through the product's installation guide and can be site specific.)

Use the following commands as an example:

```
TSS ADDTO(RDT) RESCLASS(BMCVIEW) -
RESCODE(3B) DEFACC(READ) -
ATTR(MASK|NOMASK,DEFPROT,LONG,GENERIC) -
ACLST(NONE,READ,UPDATE,ALL)
```

CCI: CCI-000336

CCI: CCI-002358

Group ID (Vulid): V-18014
Group Title: ZB000040
Rule ID: SV-37808r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZMVZT040
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.

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|TSS)

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|TSS)

CCI: CCI-000035

UNCLASSIFIED