VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

z/OS BMC IOA for TSS STIG

Version: 6

Release: 7

26 Oct 2018

XSL Release 1/29/2015 Sort by: STIGID

Group ID (Vulid): V-17985
Group Title: ZB000060
Rule ID: SV-32018r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZIOA0060
Rule Title: BMC IOA security exits are not installed or configured properly.

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

IOASE06
IOASE07
IOASE09
IOASE12
IOASE16
IOASE32
IOASE40
IOASE42

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

IOASE06
IOASE07
IOASE09
IOASE12
IOASE16
IOASE32

IOASE40
IOASE42

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-31826r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZIOAT000
Rule Title: BMC IOA installation data sets will be properly protected.

Vulnerability Discussion: BMC IOA 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(IOARPT)

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

- PDI(ZIOA0000)

Verify that the accesses to the BMC IOA 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, operations, production control and scheduling personnel, 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 IOA installation data sets are limited to System Programmers only. READ access can be given to auditors, BMC users, operations, production control and scheduling personnel, 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.*.IOAI.

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

TSS PERMIT(<syspaudt>) DSN(SYS2.IOA.*.IOAI.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<syspaudt>) DSN(SYS2.IOA.*.IOAI.) ACCESS(READ)
TSS PERMIT(<audtaudt>) DSN(SYS2.IOA.*.IOAI.) ACCESS(READ)
TSS PERMIT(<bmcuser>) DSN(SYS2.IOA.*.IOAI.) ACCESS(READ)
TSS PERMIT(<operaudt>) DSN(SYS2.IOA.*.IOAI.) ACCESS(READ)
TSS PERMIT(<pcspaudt>) DSN(SYS2.IOA.*.IOAI.) ACCESS(READ)
TSS PERMIT(BMC STCs) DSN(SYS2.IOA.*.IOAI.) ACCESS(READ)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-31948r3_rule
Severity: CAT II
Rule Version (STIG-ID): ZIOAT001
Rule Title: BMC IOA STC data sets must be properly protected.

Vulnerability Discussion: BMC IOA 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(IOASTC)

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

- PDI(ZIOA0001)

Verify that the accesses to the BMC IOA 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 BMC users.

___ The TSS data set access authorizations restrict WRITE and/or greater access to systems programming personnel.

___ The TSS data set access authorizations restrict UPDATE access to the BMC STCs, batch users and BMC administrators.

Fix Text: Ensure that WRITE and/or greater access to BMC IOA STC data sets are limited to System Programmers only. UPDATE access can be given to BMC STCs, batch users and BMC administrators. 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.

The installing Systems Programmer 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.*.IOAO.

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

TSS PERMIT(<syspaudt>) DSN(SYS3.IOA.*.IOAO.) ACCESS(ALL)
TSS PERMIT(<tstcaudt>) DSN(SYS3.IOA.*.IOAO.) ACCESS(ALL)
TSS PERMIT(BMC STCs) DSN(SYS3.IOA.*.IOAO.) ACCESS(U)
TSS PERMIT(<bmcadmin>) DSN(SYS3.IOA.*.IOAO.) ACCESS(U)
TSS PERMIT(<audtaudt>) DSN(SYS3.IOA.*.IOAO.) ACCESS(R)
TSS PERMIT(<bmcuser>) DSN(SYS3.IOA.*.IOAO.) ACCESS(R)

CCI: CCI-001499

Group ID (Vulid): V-21592
Group Title: ZB000002
Rule ID: SV-32154r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZIOAT002
Rule Title: BMC IOA User data sets will be properly protected.

Vulnerability Discussion: BMC IOA User data sets, IOA Core 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(IOAUSER)

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

- PDI(ZIOA0002)

Verify that the accesses to the BMC IOA User data sets are properly restricted.

If the following guidance is true, this is not a finding.

___ The TSS data set access authorizations restricts READ access to auditors.

___ The TSS data set access authorizations restricts WRITE and/or greater access to systems programming personnel.

___ The TSS data set access authorizations restricts WRITE and/or greater access to the BMC STCs and/or batch users.

___ The TSS data set access authorizations restricts UPDATE access to production control and scheduling personnel and the BMC users.

Fix Text: The IAO will ensure that WRITE and/or greater access to BMC IOA User data sets are limited to System Programmers and/or BMC STCs and/or batch users only. UPDATE access can be given to production control and scheduling personnel and the 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.*.IOAC.

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

TSS PERMIT(<syspaudt>) DSN(SYS3.IOA.*.IOAC.) ACCESS(ALL)
TSS PERMIT(<tstcaudt>) DSN(SYS3.IOA.*.IOAC.) ACCESS(ALL)
TSS PERMIT(BMC STCs) DSN(SYS3.IOA.*.IOAC.) ACCESS(ALL)
TSS PERMIT(<bmcuser>) DSN(SYS3.IOA.*.IOAC.) ACCESS(U)
TSS PERMIT(<pcspaudt>) DSN(SYS3.IOA.*.IOAC.) ACCESS(U)
TSS PERMIT(<audtaudt>) DSN(SYS3.IOA.*.IOAC.) ACCESS(R)

CCI: CCI-000213

Group ID (Vulid): V-17947

Group Title: ZB000020
Rule ID: SV-32066r3_rule
Severity: CAT II
Rule Version (STIG-ID): ZIOAT020
Rule Title: BMC IOA resources must be properly defined and protected.

Vulnerability Discussion: BMC IOA 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 report produced by the Data Set and Resource Data Collection:

- SENSITVE.RPT(ZIOA0020)

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

- PDI(ZIOA0020)

Verify that the accesses to resources and/or generic equivalent are properly restricted according to the requirements specified in BMC IOA 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 IOA 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($$ADDCND)
TSS PERMIT(<autoaudt>) IOA($$ADDCND) ACC(ALL)
TSS PERMIT(<operaudt>) IOA($$ADDCND) ACC(ALL)
TSS PERMIT(<pcspaudt>) IOA($$ADDCND) ACC(ALL)
TSS PERMIT(<prodaudt>) IOA($$ADDCND) ACC(ALL)
TSS PERMIT(<syspaudt>) IOA($$ADDCND) ACC(ALL)

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-32078r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZIOAT030
Rule Title: BMC IOA Started Task name must be properly identified and defined to the system ACP.

Vulnerability Discussion: BMC IOA 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)

Verify that the ACID(s) for the BMC IOA started task(s) is (are) properly defined. If the following attributes are defined, this is not a finding.

FACILITY(STC, BATCH)
PASSWORD(xxxxxxxx,0)
MASTFAC(IOA)
SOURCE(INTRDR)
NOSUSPEND

Fix Text: The IAO working with the systems programmer will ensure the BMC IOA Started Task(s) is (are) 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.

The following commands are provided as a sample for defining Started Task(s):

```
TSS CREATE(IOAGATE) TYPE(USER) -
     NAME('*STC* for IOA') DEPT(xxxx) -
    FAC(STC,BATCH) -
    MASTFAC(IOA) PASS(xxxxxxxx,0) -
    SOURCE(INTRDR) NOSUSPEND
```

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-32178r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZIOAT032
Rule Title: BMC IOA 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(ZIOA0032)

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

Fix Text: The BMC IOA 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 IOA 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(IOAGATE) ACID(IOAGATE)

CCI: CCI-000764

Group ID (Vulid): V-17469
Group Title: ZB000036
Rule ID: SV-32350r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZIOAT036
Rule Title: BMC IOA is not properly defined to the Facility Matrix Table for Top Secret.

Vulnerability Discussion: Improperly defined security controls for BMC IOA 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 IOA Facility Matrix table is defined as follows:

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

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

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

CCI: CCI-000764

Group ID (Vulid): V-18014
Group Title: ZB000040
Rule ID: SV-31960r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZIOAT040
Rule Title: BMC IOA configuration/parameter values are not specified properly.

Vulnerability Discussion: BMC IOA 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(ZIOA0040)

The following keywords will have the specified values in the BMC IOA security parameter member:

Keyword	Value
DEFMCHKI	$$IOAEDM
SECTOLI	NO
DFMI06	EXTEND
DFMI07	EXTEND
DFMI09	EXTEND
DFMI12	EXTEND
DFMI16	EXTEND
DFMI32	EXTEND
DFMI40	EXTEND
DFMI42	EXTEND
IOACLASS	IOA
TSSCLAS	ACIDCHK
IOATCBS	YES

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

Keyword	Value
DEFMCHKI	$$IOAEDM
SECTOLI	NO
DFMI06	EXTEND
DFMI07	EXTEND
DFMI09	EXTEND
DFMI12	EXTEND
DFMI16	EXTEND
DFMI32	EXTEND
DFMI40	EXTEND
DFMI42	EXTEND
IOACLASS	IOA
TSSCLAS	ACIDCHK
IOATCBS	YES

CCI: CCI-000035
