

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

zOS BMC CONTROL-M/Restart for RACF STIG

Version: 6

Release: 6

30 June 2023

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

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-31832r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCTRR000
Rule Title: BMC CONTROL-M/Restart installation data sets are not properly protected.

Vulnerability Discussion: BMC CONTROL-M/Restart 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
IACcontrols: DCSL-1, ECAR-1, ECAR-2, ECCD-1, ECCD-2

Check Content:

1. Check with your IOA or Systems Programming personnel and compile the list of

BMC CONTROL-M/Restart Installation Datasets,. Most likely they are similar to:

.SYS2.IOA.*.CTRO.** or SYS3.IOA.*.CTRO.**.

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 1. above into: "Enter fully qualified (without quotes) data set or profile name: ".

5. Hit enter.

6. Enter Y for Display covering profile?

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) .

Validate that UPDATE or higher access is limited to Systems Programming personnel. Verify Read access is given to

Auditors
BMC Users
BMC STCs
Batch Users.

10. If Conditional Access Permits: _ (E to edit data) has *data is present* next to it, place an E next to it and hit enter,Validate that conditional access permits of Update or higher are limited to Systems Programming Personnel. Verify Read access is given to:

Auditors
BMC Users
BMC STCs
Batch Users.

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

12. If 7, 8, .9 and 10 are all true, there is NO FINDING.

13. If 7, 8, .9 and 10 are not true, this is a FINDING.

Fix Text: The IAO will ensure that update and alter access to BMC

CONTROL-M/Restart 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.IOA.*.CTRO.**

SYS3.IOA.*.CTRO.**

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

```
ad 'SYS2.IOA.*.CTRO.**' uacc(none) owner(sys2) -
    audit(success(update) failures(read)) -
    data('BMC CONTROL-M/Restart Install DS')
pe 'SYS2.IOA.*.CTRO.**' id(<syspau<dt>) acc(a)
pe 'SYS2.IOA.*.CTRO.**' id(<audtaudt>) acc(r)
pe 'SYS2.IOA.*.CTRO.**' id(ControlM <bmcbatch>) acc(r)
```

```
ad 'SYS3.IOA.*.CTRO.**' uacc(none) owner(sys3) -
    audit(success(update) failures(read)) -
    data('BMC CONTROL-M/Restart Operation DS')
pe 'SYS3.IOA.*.CTRO.**' id(<syspau<dt>) acc(a)
pe 'SYS3.IOA.*.CTRO.**' id(ControlM <bmcbatch>) acc(r)
pe 'SYS3.IOA.*.CTRO.**' id(<audtaudt>) acc(r)
```

setr generic(dataset) refresh

CCI: CCI-000213

CCI: CCI002234

Group ID (Vulid): V-21592
 Group Title: ZB000002
 Rule ID: SV-32219r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCTRR002
 Rule Title: BMC CONTROL-M/Restart Archived Sysout data sets are not properly

protected.

Vulnerability Discussion: BMC CONTROL-M/Restart Archived Sysout 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
IACControls: DCSL-1, ECAR-1, ECAR-2, ECCD-1, ECCD-2

Check Content:

1. Check with your IOA or Systems Programming personnel and compile the list of BMC Control-M/Restart STC and/or batch data sets datasets,. Most likely similar to CTRSYS.**.
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?
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 production control and scheduling personnel, scheduled batch users, systems programming personnel, the BMC STC(s), and/or batch user(s). Validate that READ access is permitted to auditors and BMC 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 access is limited to production control and scheduling personnel, scheduled batch users, systems programming personnel, the BMC STC(s), and/or batch user(s). Validate that READ access is permitted to auditors and BMC Users.

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

12. If 7, 8, 9 and 10 are all true, there is NO FINDING.

13. If 7, 8, 9 and 10 are not true, this is a FINDING.

Fix Text: The IAO will ensure that update and alter access to BMC CONTROL-M/Restart Archived Sysout data sets are limited to System Programmers, the BMC CONTROL-M's STC(s), and/or batch user(s) only. Read access can be given to auditors, Production Control Scheduling personnel, and scheduled batch user(s).

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:

CTRSYS.**

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

```
ad 'CTRSYS.**' uacc(none) owner(CTRSYS) -
    data('BMC CONTROL-M/Restart Archived Sysout')
pe 'CTRSYS.**' id(<bmcbatch> CONTROLM CONTDAY) acc(a)
pe 'CTRSYS.**' id(<syspautd>) acc(a)
pe 'CTRSYS.**' id(<audtaudt> <autoaudt> <pcspautd>) acc(r)
```

setr generic(dataset) refresh

CCI: CCI-001499

UNCLASSIFIED