

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

z/OS HCD for RACF STIG

Version: 6

Release: 4

30 June 2023

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

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-30545r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZHCDR000
Rule Title: IBM Hardware Configuration Definition (HCD) install data sets
are
not properly protected.

Vulnerability Discussion: IBM Hardware Configuration Definition (HCD)
product
has the ability to use privileged functions and/or have access to
sensitive
data. Failure to properly restrict access to their 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 IBM Hardware Configuration Definition (HCD) install data sets, Likely:

1. SYS1.SCBD*.*
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. Verify that READ access to auditors, automated operations, operators, and systems programming personnel.
 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. Verify that READ access is limited to auditors, automated operations, operators, and systems programming personnel.
 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 allocate access to IBM Hardware Configuration Definition (HCD) install data sets is limited to System Programmers only, and all update and alter access is logged. Auditors, automated operations, and operators should have READ access.

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:
SYS1.SCBD*

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

```
ad 'SYS1.SCBD*.*' uacc(none) owner(sys1) -
    audit(success(update) failures(read)) -
    data('Vendor DS Profile: hcd')
pe 'SYS1.SCBD*.*' id(syspau dt tstcaudt) acc(a)
pe 'SYS1.SCBD*.*' id(audtaudt autoaudt operaudt) acc(r)
```

setr generic(dataset) refresh

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-21592
 Group Title: ZB000002
 Rule ID: SV-30598r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZHCDR002
 Rule Title: IBM Hardware Configuration Definition (HCD) User data sets are not properly protected.

Vulnerability Discussion: IBM Hardware Configuration Definition (HCD) product has the capability to use privileged functions and/or to have access to sensitive data. Failure to properly restrict access to their 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:

- a) Check with your IOA or Systems Programming personnel and compile the list IBM Hardware Configuration Definition (HCD) product user data sets, Likely:
1. The production IODF data sets. (i.e. sys3.IODFnn)
The working IODF data sets. (i.e. sys3.IODFnn.)
The activity log for the IODF data sets. (i.e. sys3.IODFnn.ACTLOG)
 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. Verify that READ access is limited to Systems Programming Personnel, auditors, Operations personnel, and Automated Operations users.
 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. Verify that READ access is limited to Systems Programming Personnel, auditors, Operations personnel, and Automated Operations users
 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.
- d) If any of the above is true, this is a FINDING.

Fix Text: The IAIO will ensure that update, and alter access to program product user data sets is limited to System Programmers and all update and allocate access is logged. Ensure that read access is limited to auditors, Operations personnel, and Automated Operations users.

The installing System Programmer will identify and document the product user 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 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:

The production IODF data sets. (i.e. hhhhhhhh.IODFnn)
 The working IODF data sets. (i.e. hhhhhhhh.IODFnn.)
 The activity log for the IODF data sets. (i.e. hhhhhhhh.IODFnn.ACTLOG)

Note: Currently on most CSD systems the prefix for these data sets is
 SYS3.IODF*.*.

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

```
ad 'sys3.iodef*.*' uacc(none) owner(sys3) -
audit(success(update) failures(read)) -
data('Vendor DS Profile: IODF for HCD )
pe 'sys3.iodef*.*' id(syspau dt tstcaudt) acc(a)
pe 'sys3.iodef*.*' id(audtaudt autoaudt operaudt) acc(r)
```

CCI: CCI-001499

Group ID (Vulid): V-17947
 Group Title: ZB000020
 Rule ID: SV-30583r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZHCDR020
 Rule Title: IBM Hardware Configuration Definition (HCD) resources are not properly defined and protected.

Vulnerability Discussion: Program products can run with sensitive system privileges, and potentially can circumvent system controls. Failure to properly control access to program 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
 IACcontrols: ECCD-1, ECCD-2

Check Content:

a) Check with your IOA or Systems Programming personnel and compile the list for

CBD resources, Likely:

1. CBD.CPC.IOCDS and CBD.CPC.IPLPARM.

2. From the Administrator Main Menu Choose Option 2 Security Server Commands

3. Choose Option: 4 General Resource Profile

4. Enter FACILITY in Class name: _____

5 . Enter Resource Profiles from a.1 (one at a time) on General Resource profile name:

_____.

6. Hit Enter.

7. Verify that the UACC is NONE

8. Verify that Audit Successes and Failures specifies UPDATE or READ for CBD.CPC.IOCDS and CBD.CPC.IPLPARM.

9. Tab down to Standard Access Permits and place an E next to it (hit enter)and

validate for

A. CBD.CPC.IOCDS and CBD.CPC.IPLPARM resources are restricted access to systems

programming and operations personnel as well as possibly any automated operations batch users with access of READ.

B. CBD.CPC.IOCDS and CBD.CPC.IPLPARM resources are restricted access to systems

programming with access of UPDATE and logged.

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 are

limited to:

A. CBD.CPC.IOCDS and CBD.CPC.IPLPARM resources are restricted access to systems

programming and operations personnel as well as possibly any automated operations batch users with access of READ.

B. CBD.CPC.IOCDS and CBD.CPC.IPLPARM resources are restricted access to systems

programming with access of UPDATE.

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

b) If items 7-10 are true for all resources in step a.1, there is NO FINDING.

c) If any items 7-10 are not true for any resource in step a.1, this is a FINDING.

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

1) The RACF rules for the CBD resource specify a default access of NONE.

2) There are no RACF rules that allow access to the CBD resource.

Example:

```
rdef facility cbd.** uacc(none) owner(admin) audit(failure(read)) -
data('added per PDI ZHCD0020')
```

3) The RACF rules for the CBD.CPC.IOCDS and CBD.CPC.IPLPARM resources are restricted access to systems programming and operations personnel as well as

possibly any automated operations batch users with access of READ.

4) The RACF rules for the CBD.CPC.IOCDS and CBD.CPC.IPLPARM resources are restricted access to systems programming with access of UPDATE and logged.

5) All RACF rules are defined with UACC(NONE).

Example:

```
rdef facility cbd.cpc.iocds.** uacc(none) owner(admin)
    audit(success(update) failures(read)) -
    data('added per PDI ZHCD0020')
rdef facility cbd.cpc.iplparm.** uacc(none) owner(admin)
    audit(success(update) failures(read)) -
    data('added per PDI ZHCD0020')
```

```
pe cbd.cpc.iocds.** cl(facility) id(syspau) acc(u)
pe cbd.cpc.iocds.** cl(facility) id(operau) acc(r)
pe cbd.cpc.iocds.** cl(facility) id(autoau) acc(r)
pe cbd.cpc.iplparm.** cl(facility) id(syspau) acc(u)
pe cbd.cpc.iplparm.** cl(facility) id(operau) acc(r)
pe cbd.cpc.iplparm.** cl(facility) id(autoau) acc(r)
```

```
setr racl(facility) ref
```

CCI: CCI-000035

CCI: CCI-002234

UNCLASSIFIED