VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

z/OS HCD for TSS STIG

Version: 6

Release: 3

20 Jan 2015

XSL Release 1/29/2015 Sort by: STIGID

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-30546r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZHCDT000
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.

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(HCDRPT)

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

- PDI(ZHCD0000)

Verify that access to the IBM Hardware Configuration Definition (HCD) install data sets are properly restricted.

___ The TSS data set rules for the data sets restricts READ access to auditors, automated operations, operators, and systems programming personnel.

___ 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 specifies that all (i.e., failures and successes) UPDATE and/or ALL access are logged.

Fix Text: The IAO will ensure that update and ALL access to IBM Hardware Configuration Definition (HCD) install data sets is limited to System Programmers only, and all update and ALL 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 ALL access and if required that all update and ALL access is logged. He will identify if any additional groups have update and/or ALL 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:

```
TSS PERMIT(audtaudt) DSN(SYS1.SCBD) ACCESS(R)
TSS PERMIT(autoaudt) DSN(SYS1.SCBD) ACCESS(R)
TSS PERMIT(operaudt) DSN(SYS1.SCBD) ACCESS(R)
TSS PERMIT(syspaudt) DSN(SYS1.SCBD) ACCESS(R)
TSS PERMIT(tstcaudt) DSN(SYS1.SCBD) ACCESS(R)
TSS PERMIT(syspaudt) DSN(SYS1.SCBD) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(tstcpaudt) DSN(SYS1.SCBD) ACCESS(ALL) ACTION(AUDIT)
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-21592
Group Title: ZB000002
Rule ID: SV-30599r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZHCDT002
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.

IAControls: DCSL-1, ECAR-1, ECAR-2, ECCD-1, ECCD-2

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

- SENSITVE.RPT(HCDUSER)

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

- PDI(ZHCD0002)

b) Verify that the access to the IBM Hardware Configuration Definition (HCD) install data sets is properly restricted. The data sets to be protected are the production and working IODF data sets as well as the activity log for the IODF data sets.

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

___ The TSS data set rules for the data sets does not restrict UPDATE and/or ALL access to systems programming personnel.

___ The TSS data set rules for the data sets does not restrict READ access to automated operations users and operations personnel.

___ The TSS data set rules for the data sets do not specify that all (i.e., failures and successes) UPDATE and/or ALL access will be logged.

c) If all of the above are untrue, there is NO FINDING.

d) If any of the above is true, this is a FINDING.

Fix Text: The IAO will ensure that update, and allocate 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:

```
TSS ADD(SYS3) DSN(SYS3)
TSS PER(syspaudt) DSN(SYS3.IODF) ACC(R)
TSS PER(tstcaudt) DSN(SYS3.IODF) ACC(R)
TSS PER(audtaudt) DSN(SYS3.IODF) ACC(R)
TSS PER(autoaudt) DSN(SYS3.IODF) ACC(R)
TSS PER(operaudt) DSN(SYS3.IODF) ACC(R)
TSS PER(syspaudt) DSN(SYS3.IODF) ACC(A) ACTION(AUDIT)
TSS PER(tstcaudt) DSN(SYS3.IODF) ACC(A) ACTION(AUDIT)
```

CCI: CCI-001499

Group ID (Vulid): V-17947
Group Title: ZB000020
Rule ID: SV-30586r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZHCDT020
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 sytems personnel with read only authority.

IAControls: ECCD-1, ECCD-2

Check Content:
a)	Refer to the following reports produced by the TSS Data Collection and Data Set and Resource Data Collection:

- TSSCMDS.RPT(WHOOIBMF)
- SENSITVE.RPT(WHOHIBMF)

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

- PDI(ZHCD0020)

b) Review the following items for the IBM Hardware Configuration Definition (HCD) resources in the IBMFAC resource class:

1) The TSS owner is defined for the CBD resource and/or IBMFAC RDT entry has DEFPROT specified.
2) There are no TSS rules that allow access to the CBD resource.
3) The TSS 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 TSS rules for the CBD.CPC.IOCDS and CBD.CPC.IPLPARM resources are restricted access to systems programming with access of UPDATE and logged.

c) If any item in (b) is untrue, this is a FINDING.

d) If all items in (b) are true, this is NOT 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 TSS owner is defined for the CBD resources and/or IBMFAC RDT entry has DEFPROT specified.

For Example:

```
TSS ADD(dept-acid)IBMFAC(CBD.)
```

```
TSS REP(RDT)RESCLASS(IBMFAC)ATTR(DEFPROT)
```

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

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.

Example:

```
TSS PERMIT(syspaudt)IBMFAC(CBD.CPC.IOCDS)ACCESS(READ)
TSS PERMIT(operaudt)IBMFAC(CBD.CPC.IOCDS)ACCESS(READ)
TSS PERMIT(autoaudt)IBMFAC(CBD.CPC.IOCDS)ACCESS(READ)
TSS PERMIT(syspaudt)IBMFAC(CBD.CPC.IOCDS) –
    ACCESS(UPDATE)ACTION(AUDIT)
TSS PERMIT(syspaudt)IBMFAC(CBD.CPC.IPLPARM)ACCESS(READ)
TSS PERMIT(operaudt)IBMFAC(CBD.CPC.IPLPARM)ACCESS(READ)
TSS PERMIT(autoaudt)IBMFAC(CBD.CPC.IPLPARM)ACCESS(READ)
TSS PERMIT(syspaudt)IBMFAC(CBD.CPC.IPLPARM) –
    ACCESS(UPDATE)ACTION(AUDIT)
```

CCI: CCI-000035

CCI: CCI-002234

UNCLASSIFIED