VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

z/OS IBM Health Checker for TSS STIG

Version: 6

Release: 2

20 Jan 2015

XSL Release 1/29/2015 Sort by: STIGID

Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-43173r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZHCKT001
Rule Title: IBM Health Checker STC data sets will be properly protected.

Vulnerability Discussion: IBM Health Checker 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(HCKSTC)

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

- PDI(ZHCK0001)

Verify that the accesses to the IBM Health Checker STC data sets are properly restricted. If the following guidance is true, this is not a finding.

___ The TSS data set rules for the data sets restricts READ access to auditors.

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

___ The TSS data set rules for the data sets restricts WRITE and/or greater access to the IBM Health Checker's STC(s) and/or batch user(s).

Fix Text: The IAO will ensure that WRITE and/or greater access to IBM Health Checker STC data sets is limited to System Programmers and/or IBM Health Checker's STC(s) and/or batch user(s) only. 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 WRITE and/or greater access

and if required that all WRITE and/or greater access is logged. He will identify if any additional groups have WRITE and/or greater 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. The dataset to be protected can be found in the HZSPROC STC member in HZSPDATA DD statement.

Data sets to be protected will be:
SYS3.*.HZSPDATA

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

TSS ADD(SYS3) DSN(SYS3)
TSS PERMIT(syspaudt) DSN(SYS3.MMG.HZSPDATA) ACCESS(ALL)
TSS PERMIT(Health Checker STCs) DSN(SYS3.MMG.HZSPDATA) ACCESS(ALL)
TSS PERMIT(audtaudt) DSN(SYS3.MMG.HZSPDATA) ACCESS(READ)

CCI: CCI-001499

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-43183r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZHCKT030
Rule Title: IBM Health Checker Started Task name will be properly identified and/or defined to the system ACP.

Vulnerability Discussion: IBM Health Checker 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)

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

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

Fix Text: The IAO working with the systems programmer will ensure the IBM Health Checker 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.

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

```
TSS CREATE(HZSPROD) TYPE(USER) -
     NAME('STC, IBM Health Checker') DEPT(xxxx) -
    FAC(STC,BATCH) PASS(xxxxxxxx,0) -
    SOURCE(INTRDR) NOSUSPEND
```

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-43188r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZHCKT032
Rule Title: IBM Health Checker Started task will be properly defined to the Started Task Table 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(ZHCK0032)

If the IBM Health Checker started task(s) is (are) defined in the TSS STC record, this is not a finding.

Fix Text: The IAO working with the systems programmer will ensure the IBM Health Checker Started Task(s) is properly identified and/or defined to the System ACP.

A unique ACID must be assigned for the IBM Health Checker started task(s) thru a corresponding STC table entry.

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

TSS ADD(STC) PROCNAME(HZSPROC) ACID(HZSPROC)

CCI: CCI-000764
