

# **VANGUARD**

**Integrity Professionals, Inc.**

---

**Enterprise Security Software**

z/OS IBM Health Checker for ACF2 STIG

Version: 6

Release: 2

29 Dec 2020

---

Group ID (Vulid): V-17067

Group Title: ZB000001

Rule ID: SV-43172r1\_rule

Severity: CAT II

Rule Version (STIG-ID): ZHCKR001

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.

Responsibility: Information Assurance Officer

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:

- SENSITIVE.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 ACF2 data set rules for the data sets restricts READ access to auditors.

\_\_\_ The ACF2 data set rules for the data sets restricts WRITE and/or greater access to systems programming personnel.

\_\_\_ The ACF2 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:

```
$KEY(S3A)
$PREFIX(SYS3)
MVA.HZSPDATA UID(syspautd) R(A) W(A) A(A) E(A)
MVA.HZSPDATA UID(Health Checker STCs) R(A) W(A) A(A) E(A)
MVA.HZSPDATA UID(audtautd) R(A) E(A)
```

CCI: CCI-001499

---

Group ID (Vulid): V-17452  
Group Title: ZB000030  
Rule ID: SV-43182r1\_rule  
Severity: CAT II  
Rule Version (STIG-ID): ZHCKR030  
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.

Responsibility: Information Assurance Officer  
IAControls: ECCD-1, ECCD-2

Check Content:

a) From the Administrator main menu, select 3;4 (Security Server Reports - General Resource Reports) and press ENTER.

b) Type 1 for General Resource Profile Summary and tab down to CLASS and enter

'STARTED' for class name.

c) Find the Health Checker General Resource profile and enter 'LR' next to it and hit ENTER. If not found go to step k below.

d) Find the userid associated with the Health Checker started task under the STDATA segment information of the Health Checker general resource profile.

e) Go back to Administrator main menu, select 3;1 (Security Server Reports User Profile) and press Enter.

f) Enter 2 (for User Attributes) and tab down to User ID and enter the User ID found in Step d) above and hit Enter.

g) If the last column on the screen (PROT) is set to "PT", the Userid has the PROTECTED attribute set. If the last column is blank, the Userid does not have the PROTECTED attribute set.

h) If PROTECTED = Yes, there is no FINDING.

i) If PROTECTED = No, there is a FINDING.

j). End Check

k) If Health Checker is NOT found as a General Resource profile under the STARTED class in

c. above, then check if is defined in the Started Procedures Table (ICHRIN03) as follows:

1. From Analyzer main Menu, go to 3;4 (Online Displays Started Procedures Analysis) and Press Enter.

2. Look for STARTED in the Source column and HZSPROC in the Procname column.

3. If the Health Checker started procedure does not have an R in the M column there is

NO FINDING (an R in the M column indicates that either the STARTED TASK USER ID does not have the protected attribute or is not defined (these are both findings) ).

4. If there is an R in the M column, there is 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.

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):

```
SET LID  
insert HZSPROC stc name('STC, IBM Health Checker')
```

CCI: CCI-000764

---

UNCLASSIFIED