

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

z/OS IBM Health Checker for RACF STIG

Version: 6

Release: 3

30 June 2023

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

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
IACcontrols: DCSL-1, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:

a) Consult with your systems programmer to identify the name of the IBM Health Checker STC dataset(s) - very likely called 'SYS3.*.HZSPDATA'. The STC dataset names can also be found on the HZSPDATA DD statement in proc HZSPROC (the Health Checker STC proc).

b) Ensure the following data set controls are in effect for the IBM Health Checker STC data sets:

- READ access to the IBM Health Checker STC data sets can be given to auditors
- UPDATE access to the IBM Health Checker STC data sets is restricted to domain level security administrators
- UPDATE or higher access to the IBM Health Checker STC data sets is restricted to systems programming personnel, the Health Checker STC and authorized batch users
- UACC (None) and NOWARNING are specified for the IBM Health Checker STC data sets
- the RACF data set rules for the IBM Health Checker STC data sets specify that all accesses of UPDATE or higher (i.e., failures and successes) are logged.

c) Verify as follows:

1. From the Administrator main menu, select 3.3 (Dataset Profile Reports) and press ENTER.
2. Tab down to the Data Set row, type LV next to the dataset profile for the IBM Health Checker STC data sets.
3. Check that UACC = None and Warning = No on the dataset profile General Information Screen.
4. Review the Standard Access List and Conditional Access List on the dataset profile General Information Screen. and verify that access is restricted as specified in b. above.
5. Verify the 'Audit Successes' and 'Audit Failures' columns on the dataset profile General Information screen . They should specify 'Successes Write' and 'Failures Write' respectively.

6. Repeat steps 1-5 above for any other IBM Health Checker dataset profiles.

d) If UPDATE and ALLOCATE (e.g. ALTER) access to the IBM Health Checker STC data sets are specified as in b. above, there is NO FINDING.

e) If UPDATE and ALLOCATE (ALTER) access to the IBM Health Checker STC data sets is not restricted as in b. above there is a FINDING.

f) If UACC = None and Warning = No there is NO FINDING

g) If UACC is not None or Warning is not No, this is a FINDING.

h) If logging is as specified in b. above there is NO FINDING.

i) If logging is not as specified in b. above, there is a FINDING.

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 Quest NC-Pass 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:

```
AD 'sys3.mmd.hzspdata.**' UACC(NONE) OWNER(SYS3) AUDIT(FAILURES(READ))

PE ' sys3.mmd.hzspdata.**' ID(syspau dt) ACC(A)
PE ' sys3.mmd.hzspdata.**' ID(Health Checker STCs) ACC(A)
PE ' sys3.mmd.hzspdata.**' ID(audtaudt) ACC(R)
```

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
IACControls: 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):

```
au HZSPROC name('STC, IBM Health Checker') owner(stc) dfltgrp(stc) nopass  
-  
    data('Health Checker')
```

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-43187r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZHCKR032
Rule Title: IBM Health Checker Started task will be properly defined to
the
STARTED resource class for RACF.

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.

Responsibility: Information Assurance Officer
IACControls: 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 (HZSPROC)..
- d). If found, there is NO FINDING.
- e) If not found, 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 found, there is NO FINDING.
4. If it is not found, 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.

A unique userid must be assigned for the IBM Health Checker started task(s) thru a corresponding STARTED class entry.

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

```
rdef started HZSPROC.** uacc(none) owner(admin) audit(all(read)) -  
    stdata(user(HXSPROC) group(stc))  
setr racl(started) ref
```

CCI: CCI-000764

UNCLASSIFIED