

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

z/OS IBM SDSF for RACF STIG

Version: 6

Release: 10

30 June 2023

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

Group ID (Vulid): V-18014
Group Title: ZB000040
Rule ID: SV-40746r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZISF0040
Rule Title: IBM System Display and Search Facility (SDSF) Configuration parameters will be correctly specified.

Vulnerability Discussion: IBM System Display and Search Facility (SDSF) ISFPARMS defines global options, panel formats, and security for SDSF. Failure to properly specify these parameter values could potentially compromise the integrity and availability of the MVS operating system and user data.

Responsibility: Systems Programmer
IACcontrols: ECCD-1, ECCD-2

Check Content:

a) Use TSO option 3.4 to review SDSFPARM DD statement in the SDSF stc.

b) If no SDSDFPARM DD statement was used look at ISFPRMxx member in the Parmlib.

(Find the applicable Parmlib by issuing F SDSF, D command).

c) Ensure the following GROUP ISFSPROG Parameters are NOT specified in the GROUP

statements:

AUTH

CMDAUTH

CMDLEV

DSPAUTH

1. Ensure a value is specified for NAME as follows:

Name(xxxxxxx)

2. If

AUTH, CMDAUTH, CMDLEV, DSPAUTH are not specified in the GROUP statements

and

a value is specified for NAME

there is NO FINDING.

3. If

AUTH, CMDAUTH, CMDLEV or DSPAUTH are specified in the GROUP statements defined in the ISFPRMxx member

or

NAME is not specified with a value

there is a FINDING.

NOTE: AUPDT is a parameter for Auto Update and allows overriding of terminal lockout times. All GROUP statements that specify a value greater than 0 for AUPDT will require justification for the setting.

Fix Text: IBM System Display and Search Facility (SDSF) system programmer will

verify that the following Global and Group function parameters appear and/or do

not appear in ISFPARMS.

For the OPTIONS statement

ATHOPEN(NO)

For each GROUP statement:

AUTH will not be specified

CMDAUTH will not be specified

CMDLEV will not be specified

DSPAUTH will not be specified

NAME a value will be specified for the NAME
 AUPDT must be specified with as value of 0

Note: AUPDT is a parameter for Auto Update and allows overriding of terminal lockout times. All GROUP statements that specify a value greater than 0 for AUPDT will require justification for the setting.

The ISFPARMS OPTIONS ATHOPEN parameter identifies how the SDSF started task allocates the HASPINDEX and SDSF menu data sets. The use of the SAF interface is consistent with the DOD requirement to control all products within the operating system using the ACP. To ensure SAF security is always in effect, review the configuration setting defined in ISFPARMS DD statement in the SDSF JCL member.

The ISFPARMS GROUP statement defines user groups and their characteristics. Some of these characteristics include access authorization to SDSF functions and commands. Access to these functions and commands can be controlled alternatively using SAF resources. The use of the SAF interface is consistent with the DOD requirement to control all products within the operating system using the ACP. To ensure SAF security is always in effect, authorizations to SDSF functions and commands should not be defined in ISFPARMS DD statement in the SDSF JCL member.

CCI: CCI-000035

Group ID (Vulid): V-16932
 Group Title: ZB000000
 Rule ID: SV-40697r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZISFR000
 Rule Title: IBM System Display and Search Facility (SDSF) installation data sets will be properly protected.

Vulnerability Discussion: IBM System Display and Search Facility (SDSF) installation 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, ECCD-1, ECCD-2

Check Content:

a) Consult with your systems programmer to identify the names of the SDSF product datasets and the data set that contains the ISFPARMS statements.

b) Ensure the following data set controls are in effect for the SDSF product data sets and the data set that contains the ISFPARMS statements:

- UPDATE or higher access to the SDSF product data sets (ISF.AISF* and ISF.SISF*) are restricted to systems programming personnel.

- UPDATE or higher access to the data sets that contains the ISFPARMS statements (identified in the SDSFPARM DD statement of the SDSF stc) is restricted to systems programming personnel.

- UACC (None) and NOWARNING are specified for the SDSF product data sets and for the data set that contains the ISFPARMS statements.

- The RACF data set rules for the SDSF data sets specify that all accesses of UPDATE or higher (i.e., failures and successes) will be logged.

c). Proceed as follows:

1. From the Administrator main menu, select 3.3 (Dataset Profile Reports) and press Enter.

2. Tab down to Data SET row, type LV next to the data set that contains the ISFPARMS statement and press ENTER.

3. Review the Universal Access and Access List

4. Repeat steps 1 -3 above for each of the SDSF product data sets.

d) If Update and Allocate (e.g. ALTER) access to the SDSF product data sets are restricted to systems programming personnel, there is NO FINDING.

e) If Update and Allocate (e.g. ALTER) access to the data sets that contain the ISFPARMS statements are restricted to systems programming personnel there is NO FINDING.,

f) If Update and Allocate (e.g. ALTER) access to the SDSF product data sets are not restricted to systems programming personnel, there is a FINDING.

g) If Update and Allocate (e.g. ALTER) access to the data sets that contain the ISFPARMS statements are not restricted to systems programming personnel, there is a FINDING.

Fix Text: The IAO will ensure that WRITE and/or greater access to IBM System Display and Search Facility (SDSF) installation data sets is limited to System Programmers only, and all WRITE and/or greater access is logged. READ access can be given to all authorized users.

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.

Data sets to be protected will be:
 SYS1.ISF.AISF
 SYS1.ISF.SISF

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

```
AD 'sys1.isf.aisf*.*' UACC(NONE) OWNER(SYS1) AUDIT(SUCCESS(UPDATE)
FAILURES(READ))
AD 'sys1.isf.sisf*.*' UACC(NONE) OWNER(SYS1) AUDIT(SUCCESS(UPDATE)
FAILURES(READ))
```

```
PE 'sys1.isf.aisf*.*' ID(syspautd) ACC(A)
PE 'sys1.isf.sisf*.*' ID(syspautd) ACC(A)
PE 'sys1.isf.sisf*.*' ID(authorized users/*) ACC(R)
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-21592
 Group Title: ZB000002
 Rule ID: SV-40731r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZISFR002

Rule Title: IBM System Display and Search Facility (SDSF) HASPINDEX data set identified in the INDEX parameter must be properly protected.

Vulnerability Discussion: IBM System Display and Search Facility (SDSF) HASPINDEX data set control the execution, configuration, and security of the SDSF products. Failure to properly protect access to these data sets could result in unauthorized access. This exposure may threaten the availability of SDSF, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer
IACcontrols: DCSL-1, ECAR-1, ECAR-2, ECCD-1, ECCD-2

Check Content:

a) Use TSO option 3.4 to browse the library/member below.

b) Ensure the following data set controls are in effect for the HASPINDEX data set specified on the INDEX control statement in the ISFPARMS member (ex.SYS1.PARMLIB(ISFPRMxx)):

All access to the HASPINDEX is restricted as follows:

. 1 Read access is restricted to auditors.

2..Update access is restricted to SDSF started tasks.

3 .Write access is restricted to systems programming personnel.

4. UACC(None) and NOWARNING is set.

c). To Verify:

1.From the Administrator main menu, review the access list for the HASPINDEX

dataset. Type 3;3 and press enter to go to

Data Set Reports.

2.Type in a 1 for DATA SET PROFILE SUMMARY, and type in the high level qualifier of the ISF profile, (e.g. ISF*), and press

Enter.

3.Tab down to the Data Set field and type in LRD and press Enter.

4. Make sure you find the name of the HASPINDEX dataset, (e.g. ISF.HASPINDEX).

5. Review the profile UACC and Access List.

d). ff (Read access is restricted to auditors

and

Update access is restricted to SDSF started tasks

and

Write access is restricted to systems programming personnel

and

UACC(NONE) and NOWARNING are specified)
for the HASPINDX dataset, then there is NO FINDING.

e) If access to the HASPINDX is not restricted to auditors, the SDSF started task and systems programming personnel as specified above, there is a FINDING.

NOTE: If running z/OS V1R11 or above, with the use of a new JES logical log, the HASPINDX may not exist and may make this vulnerability not applicable (N/A).

However if used the HASPINDX dataset must be restricted.

If running z/OS V1R11 systems or above and NOT using JES logical log, the HASPINDX data set must be protected.

Fix Text: The IAO will ensure that the HASPINDX dataset identified in the INDEX parameter value of ISFPARMS options statement is restricted as described below.

The HASPINDX data set is used by SDSF when building the SYSLOG panel. This data set contains information related to all SYSLOG jobs and data sets on the spool. Since SDSF dynamically allocates this data set, explicit user access authorization to this data set should not be required. Due to the potentially sensitive data in this data set, access authorization will be restricted.

READ access is restricted to the auditors.

UPDATE access is restricted to SDSF Started Tasks.

WRITE and/or greater access is restricted to systems programming personnel.

Note: If running z/OS V1R11 or above, with the use of a new JES logical log, the HASPINDX, may not exist and may make this vulnerability not applicable (N/A). However if used the HASPINDX dataset must be restricted.

Note: If running z/OS V1R11 systems or above and NOT using JES logical log, the HASPINDX data set must be protected.

Data sets to be protected will be:
SYS1.ISF.AISF

SYS1.ISF.SISF

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

```
AD 'sys1.haspindx.**' UACC(NONE) OWNER(SYS1) AUDIT(FAILURES(READ))
```

```
PE ' sys1.haspindx.**' ID(syspautd) ACC(A)
```

```
PE ' sys1.haspindx.**' ID(sdsf stc) ACC(U)
```

```
PE ' sys1.haspindx.**' ID(audtaudt) ACC(R)
```

CCI: CCI-001499

Group ID (Vulid): V-17947
 Group Title: ZB000020
 Rule ID: SV-40819r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZISFR020
 Rule Title: IBM System Display and Search Facility (SDSF) resources will be properly defined and protected.

Vulnerability Discussion: IBM System Display and Search Facility (SDSF) can run with sensitive system privileges, and potentially can circumvent system controls. Failure to properly control access to 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.

Documentable: YES
 Responsibility: Systems Programmer
 IAControls: ECCD-1, ECCD-2

Check Content:

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

b) Tab down to CLASS, type SDSF and press Enter.

1. Review the profiles in the Profile Name column that are listed in the SDSF

SAF resource table in the z/OS STIG Addendum.

2. Ensure that they are defined with a UACC=NONE in the UACC column:
3. If all UACCs are NONE, there is NO FINDING on this point.
4. If any UACC is not equal to NONE, this is a FINDING.
5. Check that the RACF resource logging is specified for each resource

as

specified in the SDSF SAF resource table referenced above.

c) Type LR in the CMD column of each resource name listed in the table below and check that.

1. Warning = NO
2. The Auditing options are set as defined in the SDSF SAF resource table for the resource.
3. The access list showing list of user groups, only includes valid users per the SDSF SAF resources table.
4. The users only have the level of access permitted per the SDSF SAF resource table

d) If

- WARNING is not set to NO or
- the AUDIT options for each resource are not as defined in the SDSF SAF resource table
- or any user groups are granted access who are not in the SDSF SAF resource Table
- or any users are granted access that is not permitted to them per the SDSF SAF resource table there is a FINDING.

e) If none of the conditions in d. above are true and UACC = NONE for all resource, then there is NO FINDING.

NOTE: The RACF resource access authorizations for SDSF GROUP.group-name will require additional analysis to justify access.

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

Ensure that the IBM System Display and Search Facility (SDSF) command resource access is in accordance with those outlined in SDSF SAF Resources table in the zOS STIG Addendum.

Use SDSF SAF Resources and SDSF SAF Resource Descriptions tables in the zOS STIG Addendum. These tables list the resources and access requirements for IBM System

Display and Search Facility (SDSF); ensure the following guidelines are followed:

The RACF resources and/or generic equivalent as designated in the above table are defined with a default access of NONE.

The RACF resource access authorizations restrict access to the appropriate personnel as designated in the above table.

The RACF resource logging is specified as designated in the above table.

The RACF resource rules for the resources designated in the above table specify UACC(NONE) and NOWARNING.

NOTE: The RACF resource access authorizations for SDSF GROUP.group-name will require additional analysis to justify access.

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

```
RDEFINE SDSF ISFATTR.JOBCL.** UACC(NONE) OWNER(ADMIN)
AUDIT(FAILURE(READ))
PERMIT ISFATTR.JOBCL.** CLASS(SDSF) ACCESS(UPDATE) ID(operaudt)
PERMIT ISFATTR.JOBCL.** CLASS(SDSF) ACCESS(UPDATE) ID(syspaudt)
```

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17982
Group Title: ZB000021
Rule ID: SV-40751r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZISFR021
Rule Title: IBM System Display and Search Facility (SDSF) resources will be properly defined and protected.

Vulnerability Discussion: IBM System Display and Search Facility (SDSF) can run with sensitive system privileges, and potentially can circumvent system controls. Failure to properly control access to 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: Systems Programmer
IACControls: ECCD-1

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: , type OPERCMDS and press Enter.\

c) Find profiles that begin with a prefix of server.** and server.MODIFY.mod-parm in the Profile Name column, review the corresponding UACC column

1. If all UACCs are equal to NONE, there is NO FINDING
2. If any UACC is not equal to NONE, this is a FINDING
** server here means the name of the SDSF server (likely SDSF, you can find it by going to SDSF and looking for the JOBID of the SDSF started task)

d) Type LR in the CMD column of each server.MODIFY.DISPLAY. prefixed resource and review the access list.

1. If the access list is restricted to systems programming personnel, auditors or operations personnel and their access is READ, there is NO FINDING
2. If any other user/group is on the access list, this is a FINDING

e) Type LR in the CMD column of each server.MODIFY.mod-parm. prefixed resource and review the access list.

1. If the access list is restricted to systems programming personnel and their access is CONTROL, there is NO FINDING
2. If any other user/group is on the access list, this is a FINDING

f) Review the audit values.

1. If the audit access attempts / access level value is ALL, or SUCCESS,UPDATE there is NO FINDING
2. If the audit access attempts / access level value is any other value, this is a FINDING

Note: Server is the name of the SDSF server specified either by the ISFPMAC macro or SDSF command.

mod-parm is one of the following parameters specified on the MVS MODIFY command: DEBUG, FOLDMSG, LOGCLASS, LOGTYPE, REFRESH, START, STOP, TRACE, and TRCLASS.

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

Ensure that the IBM System Display and Search Facility (SDSF) resource access is in accordance with those outlined in SDSF Server OPERCMDS Resources table in the zOS STIG Addendum.

Use SDSF Server OPERCMDS Resources table in the zOS STIG Addendum. These tables list the resources and access requirements for IBM System Display and Search Facility (SDSF); ensure the following guidelines are followed:

The RACF resources and/or generic equivalent as designated in the above table are defined with a default access of NONE.

The RACF resource access authorizations restrict access to the appropriate personnel as designated in the above table.

The RACF resource logging is specified as designated in the above table.

The RACF resource rules for the resources designated in the above table specify UACC(NONE) and NOWARNING.

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

```
RDEFINE SDSF SDSF.MODIFY.** UACC(NONE) OWNER(ADMIN)
      AUDIT(FAILURE(READ), SUCCESSFUL(UPDATE))
RDEFINE SDSF SDSF.MODIFY.DISPLAY UACC(NONE) OWNER(ADMIN)
      AUDIT(FAILURE(READ))
PERMIT SDSF.MODIFY.** CLASS(OPERCMDS) ACCESS(CONTROL) ID(syspautd)
PERMIT SDSF.MODIFY.DISPLAY CLASS(OPERCMDS) ACCESS(READ) ID(audtaudt)
PERMIT SDSF.MODIFY.DISPLAY CLASS(OPERCMDS) ACCESS(READ) ID(operaudt)
PERMIT SDSF.MODIFY.DISPLAY CLASS(OPERCMDS) ACCESS(READ) ID(syspautd)
```

CCI: CCI-000035

CCI: CCI--002234

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-40822r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZISFR030
Rule Title: IBM System Display and Search Facility (SDSF) Started Task name will be properly identified and/or defined to the system ACP.

Vulnerability Discussion: IBM System Display and Search Facility (SDSF) 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: , type STARTED for class name.
- c).Find the SDSF General Resource profile. If not found go to step 1. below.
- d). Find the userid associated with the SDSF started task under the STDATA segment information of the SDSF general resource profile.
- e). Go back to Administrator main menu, select 3;1 (Security Server Reports User Profile) and press ENTER
- f) Tab down to User ID and enter the User ID found in Step d) above and hit

enter

g). Page down till the Attributes section of the profile.

h) Verify that Protected = Yes

i) If Protected = Yes, there is no FINDING

j). If Protected = No, there is a FINDING

k). End Check

L) If SDSF 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 SDSF in the Procname column..

3. If the SDSF 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 System

Display and Search Facility (SDSF) 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 a 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 SDSF name('STC, SDSF') owner(stc) dfltgrp(stc) nopass
```

```
data('SDSF stc')
```

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-40824r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZISFR032
Rule Title: IBM System Display and Search Facility (SDSF) 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 Profiles) and press ENTER
- b) Type 1 for General Resource Profile Summary and Tab down to CLASS; enter STARTED for class name.
- c). Find the SDSF General Resource profile.
- d). If SDSF is found as a General Resource profile under the STARTED class, there is no FINDING. .
- e) If SDSF is NOT found as a General Resource profile under the STARTED class in d. 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 SDSF in the Procname

column..

3. If SDSF is not found either as a General Resource Profile under STARTED class in e. above AND not found in the Started Procedures Table, this is a FINDING.

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

A unique userid must be assigned for the IBM System Display and Search Facility (SDSF) started task(s) thru a corresponding STARTED class entry.

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

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

CCI: CCI-000764

Group ID (Vulid): V-18011
 Group Title: ZB000038
 Rule ID: SV-40831r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZISFR038
 Rule Title: IBM System Display and Search Facility (SDSF) Resource Class will be active in the RACF.

Vulnerability Discussion: Failure to use a robust ACP to control a product could potentially compromise the integrity and availability of the MVS operating system and user data.

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

Check Content:

- a) From the Analyzer main Menu, select 3 (Online Displays), press ENTER
- b) Select 7 (SETROPTS Analysis) and press ENTER
- c) Tab down and type an S next to Audit for CDT Classes, press ENTER
- d) Review the row for the SDSF class:
 - 1. If the STATUS is active, there is NO FINDING.
 - 2. If the STATUS is inactive, this is a FINDING

Fix Text: The IAO will ensure that the IBM System Display and Search Facility (SDSF) Resource Class(es) is (are) active.

Use the following commands as an example:

```
SETROPTS CLASSACT(SDSF)
```

```
CCI: CCI-000336
```

```
CCI: CCI-002358
```

UNCLASSIFIED