

# **VANGUARD**

**Integrity Professionals, Inc.**

---

**Enterprise Security Software**

z/OS IBM SDSF for ACF2 STIG

Version: 6

Release: 8

29 Dec 2020

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

IAControls: 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:

Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ATTSTC)

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

STC

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:

\$KEY(S1I)

\$PREFIX(SYS1)

ISF.AISF-- UID(syspau dt) R(A) W(L) A(L) E(A)

ISF.SISF-- UID(syspau dt) R(A) W(L) A(L) E(A)

ISF.SISF-- UID(authorized users/\*) R(A) E(A)

SET RULE

COMPILE 'ACF2.MVA.DSNRULES(S1I)' STORE

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) HASPINDX data set identified in the INDEX parameter must be properly protected.

Vulnerability Discussion: IBM System Display and Search Facility (SDSF) HASPINDX 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 HASPINDX data set specified on the INDEX control statement in the ISFPARMS member (ex.SYS1.PARMLIB(ISFPRMxx)):

All access to the HASPINDX 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 HASPINDEX dataset, then there is NO FINDING.

e) If access to the HASPINDEX 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 HASPINDEX may not exist and may make this vulnerability not applicable (N/A). However if used the HASPINDEX dataset must be restricted.

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

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:

```
$KEY(S1I)
$PREFIX(SYS1)
ISF.AISF-- UID(syspau dt) R(A) W(L) A(L) E(A)
ISF.SISF-- UID(syspau dt) R(A) W(L) A(L) E(A)
ISF.SISF-- UID(authorized users/*) R(A) E(A)
```

```
SET RULE
COMPILE 'ACF2.MVA.DSNRULES(S1I)' STORE
```

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:  
Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITVE.RPT(ZISF0020)
- ACF2CMD5.RPT(RESOURCE) Alternate report

Automated Analysis requiring additional analysis  
Refer to the following report produced by the Data Set and Resource Data

Collection:

- PDI(ZISF0020)

Ensure that all IBM System Display and Search Facility (SDSF) resources are properly protected according to the requirements specified in SDSF SAF Resources table in the z/OS STIG Addendum. If the following guidance is true, this is not a finding.

\_\_\_ The ACF2 resources and/or generic equivalent as designated in the above table are defined with a default access of NONE.

\_\_\_ The ACF2 resource access authorizations restrict access to the appropriate personnel as designated in the above table.

\_\_\_ The ACF2 resource logging is specified as designated in the above table.

\_\_\_ The ACF2 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.

(Note: The resource type, resources, and/or resource prefixes identified below are examples of a possible installation. The actual resource type, resources, and/or resource prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.)

Ensure that the IBM System Display and Search Facility (SDSF) 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 ACF2 resources and/or generic equivalent as designated in the above table are defined with a default access of NONE.

The ACF2 resource access authorizations restrict access to the appropriate personnel as designated in the above table.

The ACF2 resource logging is specified as designated in the above table.

The ACF2 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:

```
$KEY(ISFATTR) TYPE(SDS)
JOBCL.- UID(operaudt) SERVICE(READ,UPDATE) ALLOW
JOBCL.- UID(syspauudt) SERVICE(READ,UPDATE) ALLOW
- UID(*) PREVENT
```

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  
IAControls: ECCD-1

Check Content:  
Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(ZISF0021)
- ACF2CMDS.RPT(RESOURCE) Alternate report

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

- PDI(ZISF0021)

Ensure that all SDSF resources are properly protected according to the requirements specified in the SDSF Server OPERCMDS Resources table in the z/OS STIG Addendum. If the following guidance is true, this is not a finding.

\_\_\_ The ACF2 resources and/or generic equivalent as designated in the above table are defined with a default access of NONE.

\_\_\_ The ACF2 resource access authorizations restrict access to the appropriate personnel as designated in the above table.

\_\_\_ The ACF2 resource logging is specified as designated in the above table.

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 ACF2 resources and/or generic equivalent as designated in the above table are defined with a default access of NONE.

The ACF2 resource access authorizations restrict access to the appropriate personnel as designated in the above table.

The ACF2 resource logging is specified as designated in the above table.

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

```
$KEY(SDSF) TYPE(OPR)
MODIFY.DISPLAY UID(audtaudt) SERVICE(READ)
MODIFY.DISPLAY UID(operaudt) SERVICE(READ)
MODIFY.DISPLAY UID(syspauDt) SERVICE(READ)
MODIFY.- UID(syspauDt) SERVICE(READ,UPDATE,DELETE) LOG
- UID(*) PREVENT
```

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

IAControls: ECCD-1, ECCD-2

Check Content:

Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ATTSTC)

Verify that the logonid(s) for the IBM System Display and Search Facility (SDSF) started task(s) is (are) properly defined. If the following attributes are defined, this is not a finding.

STC

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):

SET LID

insert SDSF stc name('STC, SDSF')

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 defined or active in the ACP.

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:

Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMD5.RPT(ACFGSO)

If the following GSO CLASMAP record entry(ies) is (are) defined, this is not a finding.

CLASMAP.SDSF RESOURCE(SDSF) RSRCTYPE(SDS) ENTITYLN(39)

Fix Text: The IAO will use SAF security to define and protect the IBM System Display and Search Facility (SDSF) resource class(es).

Use the following commands as an example:

CLASMAP.SDSF RESOURCE(SDSF) RSRCTYPE(SDS) ENTITYLN(39)

CCI: CCI-000336

CCI: CCI-002358

---

UNCLASSIFIED