VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

z/OS IBM System Display and Search Facility (SDSF) for TSS STIG

Version: 6

Release: 8

22 Apr 2016

XSL Release 1/29/2015 Sort by: STIGID

Group ID (Vulid): V-18014
Group Title: ZB000040
Rule ID: SV-40746r5_rule
Severity: CAT II
Rule Version (STIG-ID): ZISF0040
Rule Title: IBM System Display and Search Facility (SDSF) Configuration parameters must 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.

Check Content:
Refer to the JCL procedure libraries defined to JES2 for the SDSF started task member for SDSFPARM DD statement.

Refer to the ISRPRMxx members in the logical PARMLIB concatenation.

Refer to the results of the “F SDSF,D” command. Where SDSF should specify the SDSF started task name.

Automated Analysis
Refer to the following report produced by the z/OS Data Collection:

- PDI(ZISF0040)

Ensure the following Group Parameters are specified or not specified in the GROUP statements defined in the ISFPARMS members. If the following guidance is true, this is not a finding.

For each GROUP statement:
AUPDT(0)
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

Fix Text: Ensure that the following Group function parameters appear and/or do not appear in ISFPARMS.

For each GROUP statement:
AUPDT(0)
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

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 will be controlled 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-40698r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZISFT000
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.

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

- SENSITVE.RPT(ISFRPT)

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

- PDI(ZISF0000)

Verify that the accesses to the IBM System Display and Search Facility (SDSF) installation 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 all authorized users.

___ 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 specify that all (i.e., failures and successes) WRITE and/or greater access is logged.

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:

```
TSS ADD(SYS1) DSN(SYS1)
TSS PERMIT(syspaudt) DSN(SYS1.ISF.AISF) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(syspaudt) DSN(SYS1.ISF.AISF) ACCESS(READ)
TSS PERMIT(syspaudt) DSN(SYS1.ISF.SISF) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(syspaudt) DSN(SYS1.ISF.SISF) ACCESS(READ)
TSS PERMIT(authorized users/ALL) DSN(SYS1.ISF.SISF) ACCESS(READ)
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-21592
Group Title: ZB000002
Rule ID: SV-40733r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZISFT002

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.

Check Content:
If the z/OS operating system is Release 2.2 or higher this is not applicable.

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

- SENSITVE.RPT(SDSFRPT)

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

- PDI(ZISF0002)

Verify that the accesses to the IBM System Display and Search Facility (SDSF) HASPINDX data set specified on the INDEX control statement in the ISFPARMS statements (identified in the SFSFPARM DD statement of the SDSF stc) 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 the auditors.

___ The TSS data set rules for the data sets restricts UPDATE access to SDSF Started Tasks.

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

Fix Text: 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 may be:
SYS1.HASPINDX

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

```
TSS ADD(SYS1) DSN(SYS1)
TSS PERMIT(syspaudt) DSN(SYS1.HASPINDX) ACCESS(ALL)
TSS PERMIT(sdsf stc) DSN(SYS1.HASPINDX) ACCESS(UPDATE)
TSS PERMIT(audtaudt) DSN(SYS1.HASPINDX) ACCESS(READ)
```

CCI: CCI-000213

Group ID (Vulid): V-17947
Group Title: ZB000020
Rule ID: SV-40820r5_rule
Severity: CAT II
Rule Version (STIG-ID): ZISFT020
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
IAControls: ECCD-1, ECCD-2

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

- SENSITVE.RPT(ZISF0020)

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 TSS resources and/or generic equivalent as designated in the above table are owned or DEFPROT is specified for the resource class.

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

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

___ The TSS resource access authorizations for SDSF GROUP.group-name will require additional analysis to justify access.

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

(Note: The resource class, resources, and/or resource prefixes identified below are examples of a possible installation. The resource class, actual resources, and/or 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) 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 TSS resources and/or generic equivalent as designated in the above table are owned or DEFPROT is specified for the resource class.

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

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

The TSS 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:

```
TSS ADD(dept-acid) SDSF(ISFATTR)
TSS PERMIT(operaudt) SDSF(ISFATTR.JOBCL) ACCESS(UPDATE)
TSS PERMIT(syspaudt) SDSF(ISFATTR.JOBCL) ACCESS(UPDATE)
```

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17982
Group Title: ZB000021
Rule ID: SV-40752r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZISFT021
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.

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

- SENSITVE.RPT(ZISF0021)

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 TSS resources and/or generic equivalent as designated in the above table are owned or DEFPROT is specified for the resource class.

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

___ The TSS 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 TSS resources and/or generic equivalent as designated in the above table are owned or DEFPROT is specified for the resource class.

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

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

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

```
TSS ADD(dept-acid) OPERCMDS(SDSF)
TSS PERMIT(syspaudt) OPERCMDS(SDSF.MODIFY) ACCESS(CONTROL) ACTION(AUDIT)
TSS PERMIT(audtaudt) OPERCMDS(SDSF.MODIFY.DISPLAY) ACCESS(READ)
TSS PERMIT(operaudt) OPERCMDS(SDSF.MODIFY.DISPLAY) ACCESS(READ)
TSS PERMIT(syspaudt) OPERCMDS(SDSF.MODIFY.DISPLAY) ACCESS(READ)
```

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-40823r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZISFT030
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.

Check Content:
Refer to the following report produced by the TSS Data Collection:

- TSSCMDS.RPT(@ACIDS)

Verify that the ACID(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.

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

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):

```
TSS CREATE(SDSF) TYPE(USER) -
     NAME('STC, SDSF') 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-40825r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZISFT032
Rule Title: IBM System Display and Search Facility (SDSF) Started task will be properly defined to the Started Task Table ACID 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.

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(ZISF0032)

If the IBM System Display and Search Facility (SDSF) 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 System Display and Search Facility (SDSF) Started Task(s) is properly identified and/or defined to the System ACP.

A unique ACID must be assigned for the IBM System Display and Search Facility (SDSF) 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(SDSF) ACID(SDSF)
```

CCI: CCI-000764
