VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

z/OS ICSF for TSS STIG

Version: 6

Release: 5

27 Jul 2018

XSL Release 1/29/2015 Sort by: STIGID

Group ID (Vulid): V-18014
Group Title: ZB000040
Rule ID: SV-95665r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZICS0040
Rule Title: IBM Integrated Crypto Service Facility (ICSF) Configuration parameters must be correctly specified.

Vulnerability Discussion: IBM Integrated Crypto Service Facility (ICSF) product has the ability to use privileged functions and/or have access to sensitive data. Failure to properly configure parameter values could potentially the integrity of the base product which could result in compromising the operating system or sensitive data.

Check Content:
Refer to the CSFPRMxx member in the logical PARMLIB concatenation.

If the configuration parameters are specified as follows this is not a finding.

REASONCODES(ICSF)
COMPAT(NO)
SSM(YES)
CHECKAUTH(YES)
FIPSMODE(YES,FAIL(NO))
AUDITKEYLIFECKDS (TOKEN(YES),LABEL(YES)).
AUDITKEYLIFEPKDS (TOKEN(YES),LABEL(YES)).
AUDITKEYLIFETKDS (TOKENOBJ(YES),SESSIONOBJ(YES)).
AUDITKEYUSGCKDS (TOKEN(YES),LABEL(YES),INTERVAL(n)).
AUDITKEYUSGPKDS (TOKEN(YES),LABEL(YES),INTERVAL(n)).
AUDITPKCS11USG (TOKENOBJ(YES),SESSIONOBJ(YES),NOKEY(YES),INTERVAL(n)).

DEFAULTWRAP should not be specified.

Note: Other options may be site defined.

Fix Text: Evaluate the impact associated with implementation of the control options. Develop a plan of action to implement the control options for CSFPRMxx as specified below:

REASONCODES(ICSF)
COMPAT(NO)
SSM(YES)
CHECKAUTH(YES)
FIPSMODE(YES,FAIL(NO))

AUDITKEYLIFECKDS (TOKEN(YES),LABEL(YES)).
AUDITKEYLIFEPKDS (TOKEN(YES),LABEL(YES)).
AUDITKEYLIFETKDS (TOKENOBJ(YES),SESSIONOBJ(YES)).
AUDITKEYUSGCKDS (TOKEN(YES),LABEL(YES),INTERVAL(n)).
AUDITKEYUSGPKDS (TOKEN(YES),LABEL(YES),INTERVAL(n)).
AUDITPKCS11USG (TOKENOBJ(YES),SESSIONOBJ(YES),NOKEY(YES),INTERVAL(n)).

DEFAULTWRAP should not be specified

Note: Other options may be site defined.

CCI: CCI-000035

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-30550r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZICST000
Rule Title: IBM Integrated Crypto Service Facility (ICSF) install data sets are not properly protected.

Vulnerability Discussion: IBM Integrated Crypto Service Facility (ICSF) product has the ability to use privileged functions and/or have access to sensitive data. Failure to properly restrict access to their 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:
a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITVE.RPT(ICSFRPT)

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

- PDI(ZICS0000)

b) Verify that access to the IBM Integrated Crypto Service Facility (ICSF) install data sets are properly restricted.

___ The TSS data set rules for the data sets does not restrict UPDATE and/or ALL access to systems programming personnel.

___ The TSS data set rules for the data sets does not specify that all (i.e., failures and successes) UPDATE and/or ALL access will be logged.

c) If all of the above are untrue, there is NO FINDING.

d) If any of the above is true, this is a FINDING.

Fix Text: The IAO will ensure that update and allocate access to IBM Integrated Crypto Service Facility (ICSF) install data sets is limited to System Programmers only, and all update and allocate access is logged. Read access can be given to Auditors and any other users that have a valid requirement to utilize these data sets.

The installing Systems Programmer will identify and document the product data sets and categorize them according to who will have update and alter access and if required that all update and allocate access is logged. He will identify if any additional groups have update 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.CSF

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

TSS PERMIT(syspaudt) DSN(SYS1.CSF.) ACCESS(R)
TSS PERMIT(tstcaudt) DSN(SYS1.CSF.) ACCESS(R)
TSS PERMIT(icsfusrs) DSN(SYS1.CSF.) ACCESS(R)
TSS PERMIT(syspaudt) DSN(SYS1.CSF.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(tstcaudt) DSN(SYS1.CSF.) ACCESS(ALL) ACTION(AUDIT)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-30565r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZICST001
Rule Title: IBM Integrated Crypto Service Facility (ICSF) STC data sets must be properly protected.

Vulnerability Discussion: IBM Integrated Crypto Service Facility (ICSF) STC data sets have the ability to use privileged functions and/or have access to sensitive data. Failure to properly restrict access to their 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(ICSFSTC)

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

- PDI(ZICS0001)

Verify that access to the IBM Integrated Crypto Service Facility (ICSF) STC data sets are properly restricted. The data sets to be protected are identified in the data set referenced in the CSFPARM DD statement of the ICSF started task(s) and/or batch job(s), the entries for CKDSN and PKDSN specify the data sets. If the following guidance is true, this is not a finding.

___ The TSS data set access authorizations restrict READ access to auditors.

___ The TSS data set access authorizations restrict WRITE and/or greater access to systems programming personnel.

___ The TSS data set access authorizations restrict WRITE and/or greater access to the product STC(s) and/or batch job(s).

Fix Text: The ISSO will ensure that WRITE and/or greater access to IBM Integrated Crypto Service Facility (ICSF) STC and/or batch data sets are limited to system programmers and ICSF STC and/or batch jobs only. READ access can be given to auditors at the IAOs discretion.

The installing Systems Programmer will identify and document the product data sets and categorize them according to who will have what type of access and if required which type of access is logged. The installing systems programmer will identify any additional groups requiring access to specific data sets, and once documented the installing systems programmer will work with the ISSO to see that they are properly restricted to the ACP (Access Control Program) active on the system.

(Note: The data sets and/or data set prefixes identified below are examples of a

possible installation. The actual data sets 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.)

The data sets to be protected are identified in the data set referenced in the CSFPARM DD statement of the ICSF started task(s) and/or batch job(s), the entries for CKDSN and PKDSN specify the data sets.

Note: Currently on most CSD systems the CKDSN specifies SYS3.CSF.CKDS and PKDSN specifies SYS3.CSF.PKDS.

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

TSS PERMIT(audtaudt) DSN(SYS3.CDS.) ACCESS(R)
TSS PERMIT(syspaudt) DSN(SYS3.CDS.) ACCESS(R)
TSS PERMIT(tstcaudt) DSN(SYS3.CDS.) ACCESS(R)
TSS PERMIT(icsfstc) DSN(SYS3.CDS.) ACCESS(R)
TSS PERMIT(syspaudt) DSN(SYS3.CDS.) ACCESS(ALL)
TSS PERMIT(tstcaudt) DSN(SYS3.CDS.) ACCESS(ALL)
TSS PERMIT(icsfstc) DSN(SYS3.CDS.) ACCESS(ALL)

CCI: CCI-001499

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-30591r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZICST030
Rule Title: IBM Integrated Crypto Service Facility (ICSF) Started Task name is not properly identified / defined to the system ACP.

Vulnerability Discussion: IBM Integrated Crypto Service Facility (ICSF) 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:
a) Refer to the following reports produced by the TSS Data Collection:

- TSSCMDS.RPT(@ACIDS)

b) Review the IBM Integrated Crypto Service Facility (ICSF) STC/Batch

ACID(s) for the following:

___ Is defined with Facility of STC and/or BATCH.

___ Is sourced to the INTRDR.

c) If all of the above are true, there is NO FINDING.

d) If any of the above is untrue, this is a FINDING.

Fix Text: The Systems Programmer and IAO will ensure that the started task for IBM Integrated Crypto Service Facility (ICSF) Started Task(s) is properly Identified / 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. Define the started task userid CSFSTART for IBM Integrated Crypto Service Facility (ICSF).

Example:

```
TSS CRE(CSFSTART) DEPT(Dept) NAME('ICSF STC') -
    FAC(STC) PASSWORD(password,0) -
    SOURCE(INTRDR)
```

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-30580r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZICST032
Rule Title: IBM Integrated Crypto Service Facility (ICSF) Started task(s) must 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(ZICS0032)

Verify that the IBM Integrated Crypto Service Facility (ICSF) started task(s) is (are) defined in the TSS STC record.

Fix Text: The IBM Integrated Crypto Service Facility (ICSF) system programmer and the IAO will ensure that a product's started task(s) is (are) properly identified and/or defined to the System ACP.

A unique ACID must be assigned for the IBM Integrated Crypto Service Facility (ICSF) started task(s) thru a corresponding STC table entry.

The following sample set of commands is shown here as a guideline:

TSS ADD(STC) PROCNAME(CSFSTART) ACID(CSFSTART)

CCI: CCI-000764
