



# **z/OS ICSF for RACF STIG**

**Version: 6**

**Release: 5**

**02 JAN 2020**

---

**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.

**Responsibility:** Systems Programmer

**IAControls:** n/a

**Check Content:**

The systems programmer responsible for supporting CSF will ensure that the CSF Started task is configured correctly.

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-30549r1\_rule

**Severity:** CAT II

**Rule Version (STIG-ID):** [ZICSR000](#)

**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.

**Responsibility:** Information Assurance Officer

**IAControls:** DCSL-1, ECAR-1, ECAR-2, ECCD-1, ECCD-2

**Check Content:**

- a) Check with your IOA or Systems Programming personnel and compile the list of IBM Integrated Crypto Service Facility (ICSF) install data sets, Likely:
1. SYS1.CSF.\*\*
  2. From the Administrator Main Menu choose Option 2 Security Server Commands
  3. then choose Option: 3 Data Set
  4. Type the resource names collected in option a.1 above into: Enter fully qualified (without quotes) data set or profile name:
- 
5. Hit enter.
  6. Enter Y for Display covering profile? Y
  7. Verify that the UACC is NONE
  8. Verify that Audit Successes and Failures specifies UPDATE or READ.
  9. Tab down to Standard Access Permits and place an E next to it (hit enter)and validate that UPDATE or higher access is limited to Systems Programming personnel. Verify that READ access is limited to Systems Programming Personnel and Auditors and any other users that have a valid requirement to utilize these data sets.Press F3 to return to previous screen.
  10. if CONDITIONAL ACCESS PERMITS: \_ (E to edit data) has \*data is present\* next to it, place an E next to it and validate that conditional access permits of Update or higher are limited to Systems Programming Personnel as well. Verify that READ access is limited to Systems Programming Personnel and Auditors and any other users that have a valid requirement to utilize these data sets. Press F3 to return to previous screen.
  11. Repeat steps 2 through 10 for all datasets in option a.1
- b) If a.7, a.8, a.9 and a.10 are all true, there is NO FINDING.
- c) If a.7, a.8, a.9 and a.10 are not 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:

ad 'SYS1.CSF.\*\*' uacc(none) owner(sys1) -

```
audit(success(update) failures(read)) -  
data('Vendor DS Profile: icsf')  
pe 'SYS1.CSF.**' id(syspau dt tstcaudt) acc(a)  
pe 'SYS1.CSF.**' id(icsfusrs) acc(r)  
  
ad 'sys1.csf.scsfmod0.**' owner(sys1)  
data('apf auth icsf ds') -  
audit(success(update) failures(read)) uacc(none)  
pe 'sys1.csf.scsfmod0.**' id(syspau dt tstcaudt) acc(a)  
  
setr generic(dataset) refresh
```

**CCI:** CCI-000213

**CCI:** CCI-002234

---

**Group ID (Vulid):** V-17067

**Group Title:** ZB000001

**Rule ID:** SV-30564r1\_rule

**Severity:** CAT II

**Rule Version (STIG-ID):** [ZICSR001](#)

**Rule Title:** IBM Integrated Crypto Service Facility (ICSF) STC data sets are not properly protected.

**Vulnerability Discussion:** IBM Integrated Crypto Service Facility (ICSF) STC 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.

**Responsibility:** Information Systems Security Officer

**IAControls:** DCSL-1, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

**Check Content:**

a) Check with your ISSO or Systems Programming personnel and compile the list of IBM Integrated Crypto Service Facility (ICSF) datasets 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. They are Likely:

1. SYS3.CSF.CKDS and SYS3.CSF.PKDS.
2. From the Administrator Main Menu choose Option 2 Security Server Commands
3. then choose Option: 3 Data Set
4. Type the resource names collected in option a.1 above into: Enter fully qualified (without quotes) data set or profile name:

- 
5. Hit enter.
  6. Enter Y for Display covering profile? Y
  7. Verify that the UACC is NONE
  8. Verify that Audit Successes and Failures specifies UPDATE or READ.
  9. Tab down to Standard Access Permits and place an E next to it (hit enter) and validate that UPDATE or higher access is limited to Systems Programming personnel, ICSF STC and/or batch jobs only. Verify that READ access is limited to Auditors. Press F3 to return to previous screen.
  10. if CONDITIONAL ACCESS PERMITS: \_ (E to edit data) has \*data is present\* next to it, place an E next to it and validate that conditional access permits of UPDATE or higher access is limited to Systems Programming personnel, ICSF STC and/or batch jobs only. Verify that READ access is limited to Auditors. Press F3 to return to previous screen.
  11. Repeat steps 2 through 10 for all datasets in option a.1

b) If a.7, a.8, a.9 and a.10 are all true, there is NO FINDING.

c) If a.7, a.8, a.9 and a.10 are not true, this is a FINDING.

**Fix Text:** The ISSO will ensure that update and alter 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 may be granted to auditors at the ISSOs 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 what type of access is logged. He will identify if any additional groups requiring access to specific data sets, and once documented he will work with the ISSO to see that they are properly restricted to the ACP (Access Control Program) active on the system.

The data sets to be protected are identified in the dataset 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 dataset controls:

```
ad 'sys3.csf.**' uacc(none) owner(sys3) -  
    audit(failures(read)) -  
    data('ICSF Output Data')  
pe 'sys3.csf.**' id(syspautd) acc(a)  
pe 'sys3.csf.**' id(tstcaudt) acc(a)  
pe 'sys3.csf.**' id(icsfstc) acc(a)  
pe 'sys3.csf.**' id(audtaudt) acc(r)
```

CCI: CCI-001499

---

**Group ID (Vulid):** V-17452

**Group Title:** ZB000030

**Rule ID:** SV-30590r1\_rule

**Severity:** CAT II

**Rule Version (STIG-ID):** [ZICSR030](#)

**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.

**Responsibility:** Information Assurance Officer

**IAControls:** ECCD-1, ECCD-2

**Check Content:**

1. From the Vanguard Security Solutions choose Administrator Option 1.
2. choose 3 Security Server Reports
3. choose option 1 User Profiles. Make sure you are in Live mode by typing LIVE on command line.
4. Tab down to USERID and type in CSFSTART. (CSFSTART is the userid that must be associated with the started task profile.)
5. choose option 1, User Summary and hit enter.
6. If the report displays NO USERIDS TO REPORT, this is a finding.
7. If the report displays the User CSFSTART, place a UA next to the userid. If the display does not show PT under the PROT column or shows No USERIDS to Report, then there is a Finding.
8. If the USERID exists and PT is specified in the PROT column, then there is no 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:

```
AU CSFSTART NAME('STC, ICSF') NOPASS -  
    OWNER(STC) DFLTGRP(STC) -  
    DATA('START ICSF')
```

**CCI:** CCI-000764

---

**Group ID (Vulid):** V-17454

**Group Title:** ZB000032

**Rule ID:** SV-30579r1\_rule

**Severity:** CAT II

**Rule Version (STIG-ID):** [ZICSR032](#)

**Rule Title:** IBM Integrated Crypto Service Facility (ICSF) Started task is not 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

**IAControls:** ECCD-1, ECCD-2

**Check Content:**

1. From the Vanguard Security Solutions choose option 3 Analyzer.
2. choose Option 3 Online Displays
3. choose Option 4 Started Procedures Analysis
4. Do a SORT on PROCNAME and then L CSFSTART or the name of the CSFSTART started task.
5. If the CSFSTART started task exists and does not have any Messages associated with it, there is NO FINDING.
6. If the CSFSTART started task does not exist or has Messages associated with it, there is a FINDING.

**Fix Text:** The IAO will properly define and implement the userid for IBM Integrated Crypto Service Facility (ICSF) Started Procedure.



A unique userid must be assigned for the CSFSTART started task thru a corresponding STARTED class entry.

A sample set of commands is shown here:

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

**CCI:** CCI-000764

---

**UNCLASSIFIED**