

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

z/OS RACF STIG

Version: 7

Release: 1

11 Aug 2025

XSL Release 08/11/2025 Sort by: STIGID

Description:

Group ID (Vulid): V-7516
Group Title: ZCIC0010
Rule ID: SV-7978r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZCIC0010
Rule Title: CICS system data sets are not properly protected.

Vulnerability Discussion: CICS is a transaction-processing product that provides programmers with the facilities to develop interactive applications. Unauthorized access to CICS system data sets (i.e., product, security, and application libraries) could result in the compromise of the confidentiality,

integrity, and availability of the CICS region, applications, and customer data.

Responsibility: Information Assurance Officer
IACcontrols: DCCS-1, DCCS-2, ECCD-1, ECCD-2

Check Content:
CICS Data Analysis

If the installation does not have CICS, the CICS Data Analysis section can be skipped.

Before completing STIGS ZCIC0010- ZCIC0042 please follow these instructions:

Using the CICSSIT JCL found in Appendix D in the U_zOS_STIG_INSTRUCTION.doc:

Copy the JCL to your system and ensure the following items are specified:

- a) CICS load library containing the CICS SIT is specified on the SDFHAUTH DD statement.
- b) Repeat the dump step (i.e., Step 2) for each CICS SIT.
- c) Ensure the PDS member name on the SITDUMP DD statement matches the actual SIT being dumped. This is helpful when matching dumps with specific CICS regions during the data analysis phase.
- d) Add an appropriate jobcard.
- e) Submit CICSSIT for execution. Review the job for error messages to ensure successful execution.
- f) The CICSSIT job will create the partitioned data set:
SYS3.FSO.xxxx.mmmmyyyy.CICS.RPT - This file will save each SIT dump in individual members. This data set and its members will be referenced in the CICS Data Analysis.

Collect data using the on-line ISPF facilities.

1. Create a list of sensitive CICS datasets as the basis for subsequent analysis.

- a) Allocate a partitioned dataset with LRECL(80), named sys3.fso.xxxx.mmmmyyyy.dsnlist to which a member can be added for each of the products to be analyzed. The respective members will contain the names of all of the infrastructure datasets related to that software product.
- b) Review the members for each of the CICS PROCs in the sys3.fso.xxxx.mmmmyyyy.cicsproc dataset to identify the CICS infrastructure dataset naming convention and the names of individual CICS datasets.
CICS infrastructure data set names are identified by DD names beginning with DFH. Also include any dataset name allocated by the SYSIN DD statement containing CICS system initialization

parameters.

Based on the naming convention in use, use ISPF/PDF option 3.4 data set name list (e.g., `**.*CICS*`) to obtain a comprehensive list of CICS product data sets, including installation data sets not referenced in PROCLIB members

c) Create a member in the DSNLIST dataset named CICSDSNS . Include all of the CICS infrastructure dataset names identified in step b) above. Enter each dataset name in the member on its own line and starting in column 1

This list of dataset names displayed using ISPF/PDF option 3.4 can generally be copied using copy and paste into the CICSDSNS member of the DSNLIST dataset. Any additional CICS dataset names identified in the CICSPROC dataset that do not follow the typical naming convention can then be added.

Note: There may well be datasets specified in the CICS PROC JCL that are related to other software such as Omegamon for CICS for which it may be appropriate to create an separate member in the DSNLIST dataset.

2. Collect CICS PROCLIB member lists and JCL..

1. Identify the system PROCLIB containing the JES2 PROC by referring to the MSTJCLxx member in PARMLIB. The JES2 PROC in use will be the first instance of a JES2 PROC in the dataset concatenation associated with the IEFPDSI DD statement.

2. In the JES2 PROC identify the PROCLIB datasets identified by the PROC00 DD statement.

3. Identify any dynamic PROCLIB datasets by issuing the system command: `/SD PROCLIB`

A response of NO SELECTABLE ENTRIES FOUND MATCHING SPECIFICATION indicates that no dynamic PROCLIB datasets are in use.

4. Use the ISPF Search-For Utility (ISPF 3.14) to identify any procedures used to initiate CICS execution by specifying DFHSIP as the SEARCH STRING.

5. The search must be conducted for each of the PROCLIB datasets identified in Steps 2 and 3 above. The search can be performed in batch as a single job with all of the PROCLIB datasets concatenated on the NEWDD DD statement in the same sequence that they appear on the PROC00 DD statement in the JES2 PROC.

6. The out put from the ISRSUPC program can be directed to a sequential dataset named: `sys3.fso.xxxx.mmmyyy.cicsproc.names` or be allowed to be directed to SYSOUT by default.

7. Allocate a partitioned dataset named: sys3.fso.xxxx.mmmmyyyy.cicsproc to which each of the CICS PROCs identified in Step 6 can be copied for further analysis.

8. Copy each of the CICS PROCs identified in Step 6 to the sys3.fso.xxxx.mmmmyyyy.cicsproc dataset for use during subsequent CICS analysis STIGs.

a) From the Analyzer Main Menu

1. Enter Option 4;B and press <ENTER>

2. On the Sensitive and Critical Data Sets Analysis panel, place an R, preceding User defined list .

3. Key in the name of the dataset and member that contains the list of all of the CICS infrastructure dataset names, for which the suggested name is:

```
sys3.fso.xxxx.mmmmyyyy.dsnlist(cicsdsns)
```

in the Fully qualified (without quotes) name of data set containing list: field.

4. Specify NO for the RACF Group Detail , Sort Criteria and Exceptions Only options.

5. Press <ENTER>

6. On the JCL Submit Processing panel specify Option E to edit the generated JCL and press <ENTER>

7. On the subsequent ISPF EDIT panel modify the REPORT DD statement in the Analyzer batch JCL to specify the dataset to which the Analyzer Sensitive Data Sets Report should be written. If DCB parameters are specified, the data set must be allocated with RECFM(FBA) and LRECL(133) attributes. Alternatively, you may wish to pre-allocate a PDS or PDSE with RECFM(FBA) and LRECL(133) attributes, such that individual Analyzer Reports can be created as individual members in a single dataset..

8. After making any desired changes to the generated JCL, submit the Administrator Job for execution either by entering submit on the command line of the ISPF EDIT panel or press <PF3> to return to the JCL Submit Processing panel and then specify Option S to submit the Administrator Job for execution.

b) Review the VSA report output for each data set analyzed.

UPDATE and/or ALTER access to CICS system datasets is restricted to systems programming personnel.

Note: The CICS region userids, the userids under which the CICS started Tasks execute, will also need UPDATE to many of the CICS infrastructure datasets and will need CONTROL access to CICS datasets for which the lowest level dataset name qualifier is typically DFHINTRA and DFHTEMP.

c) If (b) is true, there is NO FINDING.

d) If (b) is untrue, this is a FINDING.

Fix Text: Review the access authorizations for CICS system data sets for each region. Ensure they conform to the specifications below:

A CICS environment may include several data set types required for operation. Typically they are CICS product libraries, which are usually included in the STEPLIB concatenation but may be found in DD DFHRPL. CICS system data sets that can be identified with DFH DD statements, other product system data sets, and application program libraries. Restrict alter and update access to CICS program libraries and all system data sets to systems programmers only. Other access must be documented and approved by the IAO. The site may determine access to application data sets included in the DD DFHRPL and CICS region startup JCL according to need. Ensure that procedures are established; documented, and followed that prevents the introduction of unauthorized or untested application programs into production application systems.

CCI: CCI-001499

Group ID (Vulid): V-251
 Group Title: ZCIC0020
 Rule ID: SV-7528r2_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCIC0020

Rule Title: Sensitive CICS transactions are not protected in accordance with security requirements.

Vulnerability Discussion: Sensitive CICS transactions offer the ability to circumvent transaction level controls for accessing resources under CICS. These transactions must be protected so that only authorized users can access them. Unauthorized use can result in the compromise of the confidentiality, integrity, and availability of the operating system or customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:

- a) From Administrator Main Menu, enter Option 3;4 and press <ENTER>
- b) On the General Resource Reports panel specify Option 4 on the COMMAND line to request an Access Lists report.

Specify B for the Batch/On-line: Option.

Specify the RACF member class name used to control access to CICS transactions, (e.g. TCICSTRN) for the CLASS: Masking Criteria.

Press <ENTER>

- c) On the Processing Options panel specify Y for Explode RACF groups in access lists at end of report

Press <ENTER>

- d) On the JCL Submit Processing panel specify Option E to edit the generated JCL and press <ENTER>.

- e) On the subsequent ISPF EDIT panel modify the PRNT DD statement in the Administrator batch JCL to specify the dataset to which the Access Lists report should be written. If DCB parameters are specified the data set must be allocated with RECFM(FBA) and LRECL(133) attributes.

- f) After making any desired changes to the generated JCL, submit the Administrator Job for execution either by entering submit on the command line of the ISPF EDIT panel or press <PF3> to return to the JCL Submit Processing panel and then specify Option S to submit the Administrator Job for execution.

g) Return to the General Resource Reports panel by pressing <PF3> a sufficient number of time and then repeat steps b) through f) for the RACF group class name used to control access to CICS transactions.

If installation defined classes are used to control access to CICS transaction, then these steps, b) through f), must be repeated for each member and group class in use.

Alternatively, you may wish to produce Access List Reports for all of the member and group classes used for CICS transaction security in a single Administrator Job, with the reports written successively to a single dataset. This can be accomplished when editing the generated JCL in step b) by replicating the four Administrator control statements, beginning with the REPORT statement and ending with the REPORT(END) statement, for each member and group resource class to be reported. The CLASS(name) statement must be changed within each set of four control statements to specify the desired resource class name.

Note: If the series of reports to be produced are to be directed to a dataset, ensure that DISP=(MOD,CATLG) has been specified in the PRNT DD statement. As the output dataset is closed in response to each REPORT(END) statement encountered, failure to do so will cause each report produced to overlay the preceding report.

h) Ensure the following items are in effect for all CICS regions:

Refer to the information gathered from the CICS Systems Programmer s Worksheet in the Preliminary Information Worksheets in U_zOS_STIG_INSTRUCTION.doc.

1. Transactions listed in tables CICS CATEGORY 2 CICS AND OTHER PRODUCT TRANSACTIONS and CICS CATEGORY 4 COTS-SUPPLIED SENSITIVE TRANSACTIONS, in the z/OS STIG Addendum, are restricted to authorized personnel.

Note: The exception to this is the CEOT and CSGM transactions, which can be made available to all users.

Note: The transactions beginning with "CK" apply to regions running WebSphere MQ.

Note: Category 1 transactions are internally restricted to CICS region userids.

2. If the domain being reviewed is running MQSeries/WebSphere MQ, transactions listed in Section 4.3.4.2.11, CICS Transaction Security in the Z/OS STIG are restricted to CICS region userids, system programming personnel, and MQSeries administrators.

i) If the items mentioned in (h) are true for all CICS transaction resource classes,, there is NO FINDING.

j) If any item mentioned in (h) is untrue for a CICS transaction resource class, this is a FINDING

Fix Text: Develop a plan to implement the required changes.

1. Most transactions are protected in groups. An example would be "L2TRANS" which would contain all Category 2 transactions. L2TRANS is defined to RACF as a profile and contains all the Category 2 transactions. An example of how to implement this within RACF is shown here:

```
RDEF GCICSTRN L2TRANS UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
```

```
RALT GCICSTRN L2TRANS ADDMEM(CADP CBAM CDBC)
```

Permission to the transaction group can be accomplished with a sample command:

```
PE L2TRANS CL(GCICSTRN) id(<syspautd>)
```

Note that a refresh is generally needed to the member class. In this case TCICSTRN is the member class for GCICSTRN and a sample refresh command is

```
SETR RACL(TCICSTRN) REFRESH
```

2. Transactions groups should be defined and permitted in accordance with the CICS Transaction tables listed in the zOS STIG Addendum.

CCI: CCI-000213

Group ID (Vulid): V-302
Group Title: ZCIC0030
Rule ID: SV-7530r3_rule
Severity: CAT II
Rule Version (STIG-ID): ZCIC0030
Rule Title: CICS System Initialization Table (SIT) parameter values must be specified in accordance with proper security requirements.

Vulnerability Discussion: The CICS SIT is used to define system operation and configuration parameters of a CICS system. Several of these parameters control the security within a CICS region. Failure to code the appropriate values could result in unexpected operations and degraded security. This exposure may result in unauthorized access impacting the confidentiality, integrity, and availability of the CICS region, applications, and customer data.

Responsibility: Information Assurance Officer
IAControls: N/A

Check Content:

a) Gather from your CICS programmer the list of JCL used to start each CICS region. Generally these will be found in a proclib member.

Refer to the information gathered from the CICS Systems Programmer's Worksheet in the Preliminary Information Worksheets.

Refer to the CICS region SYSLOG - (Alternate source of SIT parameters). Be sure to process DFHSIT based on the order specified in Note 2

b) Ensure the following CICS System Initialization Table (SIT) parameter settings are specified for each CICS region:

The system initialization parameters are processed in the preceding order, with later system initialization parameter values overriding those specified earlier

1. SEC=YES

If SEC is not coded in the CICS region startup JCL, go to offset x 117 from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the security byte flag. Below are the hex and bit

settings for this flag with the external security setting in bold:

```
X 80 EQU B 10000000 EXTERNAL SECURITY REQUESTED
X 40 EQU B 01000000 RESOURCE PREFIX REQUIRED
X 10 EQU B 00010000 RACLIST class APPCLU required
X 08 EQU B 00001000 ESM INSTLN data is required
X 04 EQU B 00000100 Surrogate User Checking required
X 02 EQU B 00000010 Always enact resource check
X 01 EQU B 00000001 Always enact command check
```

2. DFLTUSER=CICSUSER | userid

If DFLTUSER is not coded in the CICS region startup JCL, go to offset x 118 from the beginning on the SIT dump (record sequence number - 6) for a length of 8 bytes. The value will be the CICS default userid.

3. XUSER=YES

If XUSER is not coded in the CICS region startup JCL, go to offset x 117 from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the security byte flag. Below are the hex and bit

settings for this flag with the surrogate user checking setting in bold:

```
X 80 EQU B 10000000 EXTERNAL SECURITY REQUESTED
X 40 EQU B 01000000 RESOURCE PREFIX REQUIRED
X 10 EQU B 00010000 RACLIST class APPCLU required
X 08 EQU B 00001000 ESM INSTLN data is required
X 04 EQU B 00000100 Surrogate User Checking required
X 02 EQU B 00000010 Always enact resource check
X 01 EQU B 00000001 Always enact command check
```

4. SNSCOPE=NONE | CICS | MVSIMAGE | SYSPLEX

If SNSCOPE is not coded in the CICS region startup JCL, go to offset x 124 from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the signon scope byte flag. Below are the hex settings for this flag:

```
X 01 EQU 1 SIGNON SCOPE = NONE
X 02 EQU 2 SIGNON SCOPE = CICS
X 03 EQU 3 SIGNON SCOPE = MVSIMAGE
X 04 EQU 4 SIGNON SCOPE = SYSPLEX
```

NOTE:SNSCOPE=NONE is only allowed with test/development regions.

5. XTRAN=YES | ssrrTRN | classname

If XTRAN is not coded in the CICS region startup JCL, go to offset x CA from the beginning on the SIT dump (record sequence number - 6)

for a length of 7 bytes. The value will be the resource class name used for that region. If XTRAN=YES is coded, c CICSTRN will be present.

6. SECPRFX=YES

If SECPRFX is not coded in the CICS region startup JCL, go to offset x 117 from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the security byte flag. Below are the hex and bit settings for this flag with the resource prefixing setting in bold:

```
X 80 EQU B 10000000 EXTERNAL SECURITY REQUESTED
X 40 EQU B 01000000 RESOURCE PREFIX REQUIRED
X 10 EQU B 00010000 RACLIST class APPCLU required
X 08 EQU B 00001000 ESM INSTLN data is required
X 04 EQU B 00000100 Surrogate User Checking required
X 02 EQU B 00000010 Always enact resource check
X 01 EQU B 00000001 Always enact command check
```

NOTE 1: If XTRAN=ssrrTRN is specified, resource prefixing (e.g. SECPRFX=YES) is not required to be enabled. Also, CICS regions cannot share the same resource class if resource prefixing is not active.

NOTE 2: CICS system initialization parameters are specified in the following ways:

- (a) In the system initialization table, loaded from a library in the STEPLIB concatenation of the CICS startup procedure.
- (b) In the PARM parameter of the EXEC PGM=DFHSIP statement of the CICS startup procedure.
- (c) In the SYSIN data set defined in the startup procedure (but only if SYSIN is coded in the PARM parameter).

c) If the SIT parameters are defined as specified in (b) for each CICS region, there is NO FINDING.

d) If any SIT parameter is not defined as specified in (b) for a CICS region, this is a FINDING.

Fix Text: Ensure that CICS System Initialization Table (SIT) parameter values are specified using the following guidance.

The system initialization parameters are processed in the following order, with later system initialization parameter values overriding those specified earlier.
CICS system initialization parameters are specified in the following ways:

In the system initialization table, loaded from a library in the STEPLIB concatenation of the CICS startup procedure.

In the PARM parameter of the EXEC PGM=DFHSIP statement of the CICS startup procedure.

In the SYSIN data set defined in the startup procedure (but only if SYSIN is coded in the PARM parameter).

SEC=YES - If SEC is not coded in the CICS region startup JCL, go to offset x 117 from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the security byte flag. Below are the hex and bit settings for this flag.

```
X 80 EQU B 10000000 External Security Requested <===
X 40 EQU B 01000000 Resource Prefix Required
X 10 EQU B 00010000 RACLIST class APPCLU required
X 08 EQU B 00001000 ESM INSTLN data is required
X 04 EQU B 00000100 Surrogate User Checking required
X 02 EQU B 00000010 Always enact resource check
X 01 EQU B 00000001 Always enact command check
```

DFLTUSER=<parameter> - If DFLTUSER is not coded in the CICS region startup JCL, go to offset x 118 from the beginning on the SIT dump (record sequence number - 6) for a length of 8 bytes. The value will be the CICS default userid.

XUSER=YES - If XUSER is not coded in the CICS region startup JCL, go to offset x 117 from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the security byte flag. Below are the hex and bit settings for this flag.

```
X 80 EQU B 10000000 External Security Requested
X 40 EQU B 01000000 Resource Prefix Required
X 10 EQU B 00010000 RACLIST class APPCLU required
X 08 EQU B 00001000 ESM INSTLN data is required
X 04 EQU B 00000100 Surrogate User Checking required <===
X 02 EQU B 00000010 Always enact resource check
X 01 EQU B 00000001 Always enact command check
```

SNSCOPE=NONE|CICS|MVSIMAGE|SYSPLEX

If SNSCOPE is not coded in the CICS region startup JCL, go to offset x 124 from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the signon scope byte flag. Ensure that users cannot sign on to more than one CICS production region within the scope of a single CICS region, a single z/OS image, or a sysplex. Below are the hex settings for this flag:

```
X 01 EQU 1 SIGNON SCOPE = NONE
X 02 EQU 2 SIGNON SCOPE = CICS
X 03 EQU 3 SIGNON SCOPE = MVSIMAGE
X 04 EQU 4 SIGNON SCOPE = SYSPLEX
```

Note: SNSCOPE=NONE is only allowed with test/development regions.

XTRAN=YES|ssrrTRN - If XTRAN is not coded in the CICS region startup JCL, go to offset x CA from the beginning on the SIT dump (record sequence number - 6) for a length of 7 bytes. The value will be the resource class name used for that region. If XTRAN=YES is coded, c CICSTRN will be present.

SECPRFX=YES - If SECPRFX is not coded in the CICS region startup JCL, go to offset x 117 from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the security byte flag. Below are the hex and bit settings for this flag with the resource prefixing setting bolded:

```
X 80 EQU B 10000000 External Security Requested
X 40 EQU B 01000000 Resource Prefix Required <<===
X 10 EQU B 00010000 RACLIST class APPCLU required
X 08 EQU B 00001000 ESM INSTLN data is required
X 04 EQU B 00000100 Surrogate User Checking required
X 02 EQU B 00000010 Always enact resource check
X 01 EQU B 00000001 Always enact command check
```

Note: If XTRAN=ssrrTRN is specified, resource prefixing (e.g., SECPRFX=YES) is not required to be enabled. Also, CICS regions cannot share the same resource class if resource prefixing is not active.

CCI: CCI-000366

Group ID (Vulid): V-44
 Group Title: ZCIC0040
 Rule ID: SV-7532r3_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCIC0040
 Rule Title: CICS region logonid(s) must be defined and/or controlled in accordance with the security requirements.

Vulnerability Discussion: CICS is a transaction-processing product that provides programmers with the facilities to develop interactive applications.

Improperly defined or controlled CICS region userids may provide an exposure and vulnerability within the CICS environment. This could result in the compromise of the confidentiality, integrity, and availability of the CICS region, applications, and customer data.

The region userid should be associated with a unique RACF userid.

Responsibility: Information Assurance Officer
 IACcontrols: N/A

Check Content:

- a) From the Analyzer Main Menu, enter Option 4;4 and press <ENTER>
- b) On the RACF Started Procedure Table Analysis panel, press <ENTER>.
- c) On the JCL Submit Processing panel specify Option E to edit the generated JCL and press <ENTER>
- d) On the subsequent ISPF EDIT panel modify the REPORT DD statement in the Analyzer batch JCL to specify the dataset to which the Analyzer RACF Started Procedure Table Analysis Report should be written. If DCB parameters are specified, the data set must be allocated with RECFM(FBA) and LRECL(133) attributes.

Alternatively, you may wish to pre-allocate a PDS or PDSE with RECFM(FBA) and LRECL(133) attributes, such that individual Analyzer Reports can be created as individual members in a single dataset.

- e) After making any desired changes to the generated JCL, submit the Administrator Job for execution either by entering submit on the command line of the ISPF EDIT panel or press <PF3> to return to the JCL Submit Processing panel and then specify Option S to submit the Administrator Job for execution.

<ENTER>

f) Refer to the information gathered from the CICS Systems Programmer Worksheet in the Preliminary Information Worksheets found in the U_zOS_STIG_INSTRUCTION.doc.

g) Ensure that the following is defined for each CICS region:

1. A unique userid is defined.
2. The Procedure is defined to the STARTED resource class with attributes of PRIVILEGED(NO) and TRUSTED(NO).

Fix Text: Review all CICS region, default, and end-user userids to ensure they are defined and controlled as required.

Ensure that the following is defined for each CICS region:

- 1) A unique userid is defined.

Use the RACF Adduser command to accomplish this. A sample command is provided here:

```
AU <cicsregionid> NAME('STC, CICS Region') DFLTGRP(STC) OWNER(STC)
```

- 2) Defined to the STARTED resource class.

Use the RACF RDEFINE command. A sample is provided here:

```
RDEF STARTED <cicsprocname>.* UACC(NONE) OWNER(ADMIN) DATA('USED TO MAP  
<cicsprocname> TO A VALID RACF USERID') STDATA(USER(=MEMBER) GROUP(STC)  
TRACE(YES))
```

CCI: CCI-000764

Group ID (Vulid): V-7119
 Group Title: ZCIC0041
 Rule ID: SV-7536r3_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCIC0041
 Rule Title: CICS default logonid(s) must be defined and/or controlled in accordance with the security requirements.

Vulnerability Discussion: CICS is a transaction-processing product that provides programmers with the facilities to develop interactive applications. An

improperly defined or controlled CICS default userid may provide an exposure and vulnerability within the CICS environment. This could result in the compromise of the confidentiality, integrity, and availability of the CICS region, applications, and customer data.

Documentable: YES

Responsibility: Information Assurance Officer

IAControls: N/A

Check Content:

a) From Administrator Main Menu, enter Option 11;4 and press <ENTER>

b) On the Data Services panel specify Option 4 on the COMMAND line to request an Tailor Administrator Batch JCL and press <ENTER>.

c) On the Batch Execution Job Statement panel supply an appropriate JOB statement for executing batch jobs and press <ENTER>

d) On the Administrator Batch Environment panel supply:

- in response to the ADMINISTRATOR JCL DSN the name of a PDS to which the customized JCL for the Administrator batch jobs should be written,

- in response to the Batch Command DSN the name of a sequential dataset that will be created during the execution of the Administrator batch jobs to contain the RACF commands generated by the batch job,

and press <ENTER>

e) Display the dataset specified as the ADMINISTRATOR JCL DSN in the preceding Step using ISPF/PDF option 3.4 data set name list and edit the member named VRARBLDJ containing JCL for the Administrator Batch REBUILD Facility.

Following the //STEP02.SYSIN DD * DD statement, replace the sample COMMAND(REBUILD GROUP) * statement with a COMMAND(REBUILD USER) * statement. Following this statement remove the sample group name of SYS1 and include a line containing each userid, beginning in column 1, used as the CICS default user for any of the CICS regions.

Save these changes and submit the VRARBLDJ Job for execution.

f) View the generated REBUILD commands for each of the CICS default user userids to ensure the following items are in effect :

1. The userid has not been granted the RACF OPERATIONS attribute.

2. No access to interactive on-line facilities (e.g., TSO) other than CICS.

3. A CICS segment has been defined and the TIMEOUT parameter is set to 15 minutes.

4. The userid is restricted from accessing all data sets and resources with the following exceptions:

a. Non-restricted CICS transactions (e.g., CESF, CESN, good morning transaction, etc.)

b. If applicable, resources necessary to operate in an intersystem communication (ISC) environment (i.e., LU6.1, LU6.2), and/or CICS multi-region environment (MRO)

g) If (f) is true for all CICS default userids, there is NO FINDING

h) If (f) is untrue for any CICS default userid, there is a FINDING.

i) NOTE: A system's default time for terminal lock-out or session termination

may

be lengthened to 30 minutes at the discretion of the IAM. The IAM will maintain

the documentation for each system with a time-out adjusted beyond the 15-minute

recommendation to explain the basis for this decision

Fix Text: Ensure the following items are in effect for the CICS default userid

(i.e., DFLTUSER=default userid):

1) Not granted the RACF OPERATIONS attribute.

a) Issue a RACF LU (Listuser) command on the CICS default userid.

b) The OPERATIONS attribute can be removed via the RACF command ALU <cicsdefaultuser> NOOPERATIONS

2) No access to interactive on-line facilities (e.g., TSO) other than CICS.

a) Use the RACF ALU (Altuser) command to remove attributes such as TSO. Example:

ALU <cicsdefaultuser> NOTSO

3) TIMEOUT parameter in the CICS segment is set to 15 minutes.

4) A system's default time for terminal lock-out or session termination

may be lengthened to 30 minutes at the discretion of the IAM. The IAM will

maintain the documentation for each system with a time-out adjusted beyond the 15-minute recommendation to explain the basis for this decision.

a) Use the RACF LU (ListUser) command to display the CICS segment. An example is shown here:

```
LU <cicsdefaultuser> CICS
```

b) Use the RACF ALU command to set the 15 minute timeout value. An example is shown here:

```
ALU <cicsdefaultuser> CICS(TIMEOUT(15))
```

5) Restricted from accessing all data sets and resources with the following exceptions:

a) Delete the CICS default user from dataset access lists via the command:

```
PE '<dataset profile name>' ID(<cicsdefaultuser>) DEL
```

(a) Non-restricted CICS transactions (e.g., CESF, CESN, good morning transaction, etc.)

(b) If applicable, resources necessary to operate in an intersystem communication (ISC) environment (i.e., LU6.1, LU6.2, and MRO)

NOTE: Execute the JCL in CNTL(IRRUT100) using the CICS default userid as SYSIN input. This report lists all occurrences of this userid within the RACF database, including data set and resource access lists.

c) If all items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

CCI: CCI-000764

Group ID (Vulid): V-7120
 Group Title: ZCIC0042
 Rule ID: SV-7540r2_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCIC0042
 Rule Title: CICS logonid(s) do not have time-out limit set to 15 minutes.

Vulnerability Discussion: CICS is a transaction-processing product that provides programmers with the facilities to develop interactive applications.

Improperly defined or controlled CICS region userids may provide an exposure and vulnerability within the CICS environment. This could result in the compromise of the confidentiality, integrity, and availability of the CICS region, applications, and customer data.

RACF provides the PROPCNTL class to prevent userids such as the CICS region userid from being propagated/used by unauthorized userids.

Documentable: YES

Responsibility: Information Assurance Officer

IACcontrols: N/A

Check Content:

a) From Administrator Main Menu, enter Option 3;5 and press <ENTER>

b) On the Profile Segment Reports panel specify Option 3 on the COMMAND line to request a CICS User Segment report.

Specify B for the Batch/On-line: Option (make sure Data is on Extract, not live, mode).

Press <ENTER>

c) On the JCL Submit Processing panel specify Option E to edit the generated JCL and press <ENTER>.

d) On the subsequent ISPF EDIT panel modify the PRNT DD statement in the Administrator batch JCL to specify the dataset to which the Access Lists report should be written. If DCB parameters are specified the data set must be allocated with RECFM(FBA) and LRECL(133) attributes.

e) After making any desired changes to the generated JCL, submit the Administrator Job for execution either by entering submit on the command line of the ISPF EDIT panel or press <PF3> to return to the JCL Submit Processing panel and then specify Option S to submit the Administrator Job for execution.

f) Ensure that all userids with a CICS segment have the TIMEOUT parameter set to 15 minutes.

g) If (f) is true for each CICS user, there is NO FINDING.

NOTE: If the time-out limit is greater than 15 minutes, and the system is

processing unclassified information, review the following items. If any of these is true, there is NO FINDING.

h) If a session is not terminated, but instead is locked out after 15 minutes of inactivity, a process must be in place that requires user identification and authentication before the session is unlocked. Session lock-out will be implemented through system controls or terminal screen protection.

i) A system's default time for terminal lock-out or session termination may be lengthened to 30 minutes at the discretion of the IAM. The IAM will maintain the documentation for each system with a time-out adjusted beyond the 15-minute recommendation to explain the basis for this decision.

j) The IAM may set selected userids to have a time-out of up to 60 minutes in order to complete critical reports or transactions without timing out. Each exception must meet the following criteria:

k) The time-out exception cannot exceed 60 minutes.

l) A letter of justification fully documenting the user requirement(s) must be submitted and approved by the site IAM. In addition, this letter must identify an alternate means of access control for the terminal(s) involved (e.g., a room that is locked at all times, a room with a cipher lock to limit access, a password protected screen saver set to 30 minutes or less, etc.).

m) The requirement must be revalidated on an annual basis.

n) If the CICS time-out limit is not specified for 15 minutes of inactivity, and the previously mentioned exceptions do not apply, this is a FINDING.

Fix Text: Review all CICS region, default, and end-user userids to ensure they

are defined and controlled as required.

Ensure that all userids with a CICS segment have the TIMEOUT parameter set to 15 minutes.

Examples: Use the RACF ALtUser command to assign the required value:

```
ALU <cics user> CICS(TIMEOUT(15))
```

CCI: CCI-000057

Group ID (Vulid): V-301
 Group Title: ZCICR021
 Rule ID: SV-301r2_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCICR021
 Rule Title: External RACF Classes are not active for CICS transaction checking.

Vulnerability Discussion: Implement CICS transaction security by utilizing two distinct and unique RACF resource classes (i.e., member and grouping) within each CICS region. If several CICS regions are grouped in an MRO environment, it is permissible for those grouped regions to share a common pair of resource classes. Member classes contain a RACF discrete profile for each transaction. Grouping classes contain groups of transactions requiring equal protection under RACF. Ideally, member classes contain no profiles, and all transactions are defined by groups in a grouping class.

If CICS Classes are not active, this could result in the compromise of the confidentiality, integrity, and availability of the CICS region, applications, and customer data.

Responsibility: Information Assurance Officer
 IACControls: DCCS-1, DCCS-2, 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 CCICSCMD and press Enter.

1 Review the profiles in the Profile Name column that are listed in the CICS SPI 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 CICS SPI resource table and if the logging is as

specified in

the resource table, there is NO FINDING on this point,

6. If the logging is not as specified in the CICS SPI resource table, this is a

FINDING.

c) Type LR in the CMD column of each resource name found in b. above and verify that:

1. Warning = NO

2. The access list showing list of user groups, only includes valid users per

the CICS SPI resources table.

3. The users only have the level of access permitted per the CICS SPI resource table

d) If

- WARNING is not set to NO

- or any user groups are granted access who are not in the CICS SPI resource

Table

- or any users are granted access that is not permitted to them per the CICS

SPI

resource table there is a FINDING.

e). If

- WARNING is set to NO

and

- there are no user groups granted access who are not in the CICS SPI resource

Table

and

- no users are granted access that is not permitted to them per the CICS SPI

resource table there is NO FINDING.

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 CICS Transaction Server command resource access is in accordance with those outlined in CICS SPI Resources table in the zOS STIG Addendum.

Use CICS SPI Resources and CICS SPI Resources Descriptions tables in the zOS STIG Addendum. These tables list the resources and access requirements for IBM CICS Transaction Server; 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 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 CCICSCMD ASSOCIATION.** UACC(NONE) OWNER(ADMIN)
AUDIT(FAILURE(READ))
PERMIT ASSOCIATION.** CLASS(CCICSCMD) ACCESS(READ) ID(cicsaudt)
PERMIT ASSOCIATION.** CLASS(CCICSCMD) ACCESS(READ) ID(cicuaudt)
PERMIT ASSOCIATION.** CLASS(CCICSCMD) ACCESS(READ) ID(syscaudt)
```

CCI: CCI-000213

Group ID (Vulid): V-6898
 Group Title: ZCICR041
 Rule ID: SV-7193r2_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCICR041
 Rule Title: CICS regions are improperly protected to prevent unauthorized propagation of the region userid.

Vulnerability Discussion: CICS is a transaction-processing product that provides programmers with the facilities to develop interactive applications. Improperly defined or controlled CICS userids (i.e., region, default, and terminal users) may provide an exposure and vulnerability within the CICS environment. This could result in the compromise of the confidentiality, integrity, and availability of the CICS region, applications, and customer data.

Responsibility: Information Assurance Officer
IACcontrols: DCCS-1, DCCS-2, ECSD-1, ECSD-2

Check Content:

- a) From Administrator Main Menu, enter Option 3;4 and press <ENTER>
- b) On the General Resource Reports panel specify Option 1 on the COMMAND line to request a General Resource Profile Summary report.

Specify B for the Batch/On-line: Option.

Specify the PROPCNTL class name for the CLASS: Masking Criteria.

Press <ENTER>

Note: Administrator may have to be in Extract mode in order for the batch option to work. If it does not allow a batch transaction, put EXTRACT in the command line and <ENTER>. Then enter in the data from step b again.

- c) On the JCL Submit Processing panel specify Option E to edit the generated JCL and press <ENTER>.

- d) On the subsequent ISPF EDIT panel modify the PRNT DD statement in the Administrator batch JCL to specify the dataset to which the Access Lists report should be written. If DCB parameters are specified the data set must be allocated with RECFM(FBA) and LRECL(133) attributes.

- e) After making any desired changes to the generated JCL, submit the Administrator Job for execution either by entering submit on the command line of the ISPF EDIT panel or press <PF3> to return to the JCL Submit Processing panel and then specify Option S to submit the Administrator Job for execution.

- f) Compare the results from the generated report to the data gathered from the CICS Systems Programmer's Worksheet in the Preliminary Information Worksheets, U_zOS_STIG_INSTRUCTION.doc.

- g) Check that each CICS region userid is defined as a profile name in the PROPCNTL resource class

- h) If (g) is true for every CICS region userid, there is NO FINDING,

- i) If (g) is untrue for any CICS region userid, this is a FINDING.

Fix Text: Utilize propagation control for each CICS region.

Under no circumstance should a user's batch job submitted from a CICS region execute under that CICS region's userid. To prevent this from occurring, define a profile in the PROPCNTL resource class for each CICS region. The following is an example:
RDEFINE PROPCNTL <cics-region-userid> OWNER(ADMIN) AUDIT(ALL(READ))

The PROPCNTL class must be active and RACLISTed for this protection to be in effect:
SETROPTS CLASSACT(PROPCNTL) RACLIST(PROPCNTL)

CCI: CCI-000213

UNCLASSIFIED