

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

z/OS CL/SuperSession for RACF STIG

Version: 6

Release: 11

14 Sep 2021

XSL Release 5/15/2012 Sort by: STIGID
Description:

Group ID (Vulid): V-224461
Group Title: ZB000040
Rule ID: SV-27197r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCLS0040
Rule Title: CL/SuperSession profile options are set improperly.

Vulnerability Discussion: Product configuration/parameters control the security and operational characteristics of products. If these parameter values are improperly specified, security and operational controls may be weakened. This exposure may threaten the availability of the product applications, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer
IAControls: ECCD-1, ECCD-2

Check Content:

a) The following steps are necessary for reviewing the CL/SUPERSESSION options:

1. Request on-line access from the site administrator to view CL/SUPERSESSION parameter settings.
2. Once access to the CL/SUPERSESSION Main Menu has been obtained, select the option for the ADMINISTRATOR menu.
3. From the ADMINISTRATOR menu, select the option for the PROFILE SELECTION menu.
4. From the PROFILE SELECTION menu, select the View GLOBAL Profile option.
5. After selection of the View GLOBAL Profile option, the Update GLOBAL Profile menu appears. From this menu select the profile to be reviewed:
 - a. To view the Common profile select: _Common
 - b. To view the SUPERSESSION profile select: _SupSess

b) Compare the security parameters as specified in the Required CL/Supersession Common Profile Options and Required CL/Supersession Profile Options Tables in the z/OS STIG Addendum against the CL/Supersession Profile options.

c) If all options as specified in the Required CL/Supersession Common Profile Options and Required CL/Supersession Profile Options Tables in the z/OS STIG Addendum are in effect, there is NO FINDING.

d) If any of the options as specified in the Required CL/Supersession Common Profile Options and Required CL/Supersession Profile Options Tables in the z/OS STIG Addendum is not in effect, this is a FINDING.

Fix Text: The Systems Programmer and IAO will review all session manager security parameters and control options for compliance with the requirements of the z/OS STIG Addendum Required CL/Supersession Common Profile Options and Required CL/Supersession Profile Options Tables. Verify that the options are set properly.

CCI: CCI-000035

Group ID (Vulid): V-224462
Group Title: ZB000041
Rule ID: SV-27198r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCLS0041
Rule Title: CL/SuperSession is not properly configured to generate SMF records for audit trail and accounting reports.

Vulnerability Discussion: Product configuration/parameters control the security and operational characteristics of products. If these parameter values are improperly specified, security and operational controls may be weakened. This exposure may threaten the availability of the product applications, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer
IAControls: ECCD-1, ECCD-2

Check Content:

a) Review the Network Accounting Facility (NAF) definition member of the following RLSPARM initialization parameter library:

SYS3.OMEGAMON.qualifier.RLSPARM(KLVINNAF)

Locate the SMF= parameter and determine what SMF number is used.

b) If the SMF= field specifies an SMF record number use Vanguard s Analyzer product to determine if this SMF number is being recorded in SMF:

1. From Analyzer main Menu, go to 3;H; Press <ENTER>
2. From Analyzer SMF Environment Analysis panel, key in RTYPE on the command line; Press <ENTER>
3. Scroll down to the SMF record number you are looking for. If it is not found then it is not being recorded.

c) If SMF is writing the record number specified by SMF=, there is NO FINDING.

d) If the SMF= field does not specify an SMF record number, or SMF is not writing the record number specified by SMF=, this is a FINDING.

Reference: OS/390 STIG 6.2 (10)

Fix Text: The Systems Programmer and IAO will review all session manager security parameters and control options for compliance. To ensure that the Session Manager generates SMF records for audit trail and accounting reports.

To provide an audit trail of user activity in CL/SuperSession, configure the Network Accounting Facility (NAF) to require SMF recording of accounting and audit data. Accounting to the journal data set is optional at the discretion of the site. To accomplish this, configure the following NAF startup parameters in the KLVINNAF member of the RLSPARM initialization parameter library as follows:

DSNAME= dsname Name of the NAF journal data set. Required only if the site is collecting accounting and audit data in the journal data set in addition to the SMF data.

MOD If the journal data set is used, this parameter should be set to ensure that logging data in the data set is not overwritten.

SMF=nnn SMF record number. This field is mandatory to ensure that CL/SuperSession data is always written to the SMF files.

CCI: CCI-000035

Group ID (Vulid): V-224463
Group Title: ZB000000
Rule ID: SV-27091r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCLSR000
Rule Title: CL/SuperSession Install data sets must be properly protected.

Vulnerability Discussion: CL/SuperSession Install data sets provide the capability 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

CL/Supersession Installation Datasets, Likely:

1. hlq.omegamon.**

hlq.omegamon.*.tlsload.**

hlq.omegamon.*.tlvload.**

hlq.omegamon.rlsload.**

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 either 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

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.

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: Ensure that update and allocate access to CL/SuperSession install data

sets are limited to system programmers only and all update and allocate access

is logged. Auditors should be granted READ access.

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 ISSO to see that they are properly restricted to the ACP (Access Control Program) active on the system.

The following dataset are an example of data sets to be protected:
sys2.omegamon.** /* product datasets */
sys2.omegamon.*.tlsload.**
sys2.omegamon.*.tlvload.**
sys3.omegamon.**
sys3.omegamon.rlsload.**

The following commands are provided as an example for implementing dataset controls:

```
ad 'sys2.omegamon.**' uacc(none) owner(sys2) -  
audit(success(update) failures(read) -  
data('vendor DS Profile CL/Supersession')  
pe 'sys2.omegamon.**' id(syspautd) acc(a)  
pe 'sys2.omegamon.**' id(audtaudt)  
ad 'sys2.omegamon.*.tlsload.**' uacc(none) owner(sys2) -  
audit(success(update) failures(read) -  
data('vendor DS fully qualified apf Profile CL/Supersession')  
pe 'sys2.omegamon.*.tlsload.**' id(syspautd) acc(a)  
pe 'sys2.omegamon.*.tlsload.**' id(audtaudt) ad  
'sys2.omegamon.*.tlvload.**'  
uacc(none) owner(sys2) -  
audit(success(update) failures(read) -  
data('vendor DS fully qualified apf Profile CL/Supersession')  
pe 'sys2.omegamon.*.tlvload.**' id(syspautd) acc(a)  
pe 'sys2.omegamon.*.tlvload.**' id(audtaudt)  
ad 'sys3.omegamon.**' uacc(none) owner(sys3) -  
audit(success(update) failures(read) -  
data('vendor DS Profile CL/Supersession')  
pe 'sys3.omegamon.**' id(syspautd) acc(a)  
pe 'sys3.omegamon.**' id(audtaudt)  
ad 'sys3.omegamon.rlsload.**' uacc(none) owner(sys3) -  
audit(success(update) failures(read) -  
data('site DS fully qualified apf Profile CL/Supersession')  
pe 'sys3.omegamon.rlsload.**' id(syspautd) acc(a)  
pe 'sys3.omegamon.rlsload.**' id(audtaudt)
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-224464
Group Title: ZB000001

Rule ID: SV-27097r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZCLSR001

Rule Title: CL/SuperSession STC data sets are not properly protected.

Vulnerability Discussion: CL/SuperSession STC data sets provide the capability 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, ECAR-3, ECCD-1, ECCD-2

Check Content:

a) Check with your IOA or Systems Programming personnel and compile the list of

CL/SuperSession STC datasets, Likely:

1. hlq.OMEGAMON.RLSNAM

hlq.OMEGAMON.RLSTDB

hlq.OMEGAMON.RLSVLOG

hlq.OMEGAMON.RLSNAF

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. 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, STC(s), and/or Batch Jobs. Validate that READ access is permitted to

Auditors and Authorized Users.

9. 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, STC(s), and/or Batch Jobs. Validate that READ access is permitted to Auditors

and Authorized Users.

10. 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: Ensure that WRITE and/or greater access to CL/SuperSession STC data sets are limited to system programmers and CL/SuperSession STC only. Read access can be given to auditors and 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 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 following are an example of data sets to be protected:

SYS3.OMEGAMON.RLSNAF
SYS3.OMEGAMON.RLSNAM
SYS3.OMEGAMON.RLSTDB
SYS3.OMEGAMON.RLSVLOG

The following commands are provided as an example for implementing dataset controls:

```
ad 'sys3.omegamon.rlsnaf.** uacc(none) owner(sys3) -  
audit(failures(read)) -  
data('Site Customized CL/Supersession VSAM')  
pe 'sys3.omegamon.rlsnaf.**' id(syspau dt) acc(a)  
pe 'sys3.omegamon.rlsnaf.**' id(kls) acc(a)  
pe 'sys3.omegamon.rlsnaf.**' id(audtaudt) acc(r)  
pe 'sys3.omegamon.rlsnaf.**' id(*) acc(r)
```

```
ad 'sys3.omegamon.rlsnam.** uacc(none) owner(sys3) -  
audit(failures(read)) -  
data('Site Customized CL/Supersession VSAM')  
pe 'sys3.omegamon.rlsnam.**' id(syspau dt) acc(a)  
pe 'sys3.omegamon.rlsnam.**' id(kls) acc(a)  
pe 'sys3.omegamon.rlsnam.**' id(audtaudt) acc(r)
```



```

pe 'sys3.omegamon.rlsnam.**' id(*) acc(r)

ad 'sys3.omegamon.rlstdb.** uacc(none) owner(sys3) -
audit(failures(read)) -
data('Site Customized CL/Supersession VSAM')
pe 'sys3.omegamon.rlstdb.**' id(syspau dt) acc(a)
pe 'sys3.omegamon.rlstdb.**' id(kls) acc(a)
pe 'sys3.omegamon.rlstdb.**' id(audtaud t) acc(r)
pe 'sys3.omegamon.rlstdb.**' id(*) acc(r)

ad 'sys3.omegamon.rlsvlog.** uacc(none) owner(sys3) -
audit(failures(read)) -
data('Site Customized CL/Supersession VSAM')
pe 'sys3.omegamon.rlsvlog.**' id(syspau dt) acc(a)
pe 'sys3.omegamon.rlsvlog.**' id(kls) acc(a)
pe 'sys3.omegamon.rlsvlog.**' id(audtaud t) acc(r)
pe 'sys3.omegamon.rlsvlog.**' id(*) acc(r)

```

CCI: CCI-001499

Group ID (Vulid): V-224465
 Group Title: ZB000030
 Rule ID: SV-28591r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCLSR030
 Rule Title: CL/Supersession Started Task name is not properly identified
 /
 defined to the system ACP.

Vulnerability Discussion: CL/Supersession 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:

a) Use Vanguard s Analyzer product to look at the Started Procedures
 Analysis
 report:

a. From Analyzer main Menu, go to 3;4; Press <ENTER>
 b. Key in SORT PROCNAME; Press <ENTER>

- c. Key in L KLS; Press <ENTER>
 - d. If not found then KLS is not defined to RACF as a STC user.
 - e. If found then you would use the U line command to determine if the userid is defined to RACF.
 - f. Key the U line command for the KLS entry; Press <ENTER>
 - g. The userid is defined to RACF if a userid display appears. If not defined
you should see the message Unable to display .
- b) If the userid for the CL/SUPERSESSSION started task is defined to the security database, there is NO FINDING.
- c) If the userid for the CL/SUPERSESSSION started task is not defined to the security database, this is a FINDING.

Reference: OS/390 STIG 6.2.2 (3)

Fix Text: The Systems Programmer and IAO will ensure that the started task for CL/Supersession is properly defined.

Review all session manager security parameters and control options for compliance. Develop a plan of action and implement the changes as specified.

Define the started task userid KLS for CL/Supersession.

Example:

```
AU KLS NAME('STC, SUPERSESSSION') NOPASS -  
  OWNER(STC) DFLTGRP(STC) -  
  DATA('START CL SUPERSESSSION')
```

CCI: CCI-000764

Group ID (Vulid): V-224466
Group Title: ZB000032
Rule ID: SV-27191r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCLSR032
Rule Title: The CL/Supersession 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:

a) Use Vanguard s Analyzer product to look at the Started Procedures Analysis report:

1. From Analyzer main Menu, go to 3;4; Press <ENTER>
2. Key in SORT PROCNAME; Press <ENTER>
3. Key in L KLS or the name of the KLS started procedure; Press <ENTER>
4. Look at the source column. It will indicate STARTED class profile or ICHRIN03 entry.
5. If not found then the KLS started procedure is not defined to RACF as an STC user.

b) If a STARTED resource class profile exists for the CL/SUPERSESSION started task KLS, there is NO FINDING.

c) If neither a STARTED resource class profile or an ICHRIN03 entry exists for the CL/SUPERSESSION started task KLS, this is a FINDING.

Reference: OS/390 STIG 6.2.2 (2)

Fix Text: Review all session manager security parameters and control options for compliance. Develop a plan of action and implement the changes as specified.

The following command list gives an example of defining a STARTED class profile for the KLS Started Procedure userid:

```
RDEF STARTED KLS.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
STDATA(USER(KLS)
GROUP(STC) TRACE(YES)) DATA('USE THE KLS USERID TO RUN THE SUPERSESSION
PROC')
```

CCI: CCI-000764

Group ID (Vulid): V-224467
Group Title: ZB000038
Rule ID: SV-27189r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCLSR038
Rule Title: CL/SuperSession's Resource Class is not 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:

a) Use Vanguard's Analyzer product to look at the RACF SETROPTS settings:

1. From Analyzer main Menu, go to 3;1; Press <ENTER>
2. Scroll down to the CLASS information you are looking for. If you cannot find the class then it is not defined to RACF. If you find it the display will indicate whether or not the class is active or inactive.

b) If the resource class of APPL is active, there is NO FINDING.

c) If the resource class of APPL is not active, this is a FINDING.

Reference: OS/390 STIG 6.2.2 (7)

Fix Text: 1. Ensure that the APPL class is active:

```
SETROPTS CLASSACT(APPL)
```

2. With dynamic application lists enabled, only applications authorized to the

user are displayed on the session menu at the terminal. Ensure that all applications defined to CL/SUPERSESSION are defined to the APPL resource class with a default access of none.

The resource names are VTAM network names (APPLIDs). For example:

```
RDEFINE APPL applid UACC(NONE) OWNER(admin) AUDIT(ALL(READ))
```

3. Permit access to applications based on users responsibilities and roles. For example:

```
PE applid CLASS(APPL) ID(authorized-group)
```

CCI: CCI-000336

CCI: CCI-002358

Group ID (Vulid): V-224468
Group Title: ZB000042
Rule ID: SV-27257r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCLSR042
Rule Title: CL/SuperSession KLVINNAM member is not configured in accordance with the proper security requirements.

Vulnerability Discussion: Product configuration/parameters control the security and operational characteristics of products. If these parameter values are improperly specified, security and operational controls may be weakened. This exposure may threaten the availability of the product applications, and compromise the confidentiality of customer data.

Responsibility: Systems Programmer
IAControls: ECCD-1, ECCD-2

Check Content:

a) Review the member KLVINNAM in SYS3.OMEGAMON.qualifier.RLSPARM of the RLSPARM initialization parameter library.

b) If the parameters for member KLVINNAM are configured as below (either parameter set 1 or parameter set 2) , there is NO FINDING:

Parameter Set 1:
DEFAULT DSNAME(SYS3.OMEGAMON.qualifier.RLSNAM) RACF -

NODB CLASSES=APPCLASS
Parameter Set 2:
DEFAULT DSNAME(SYS3.OMEGAMON.qualifier.RLSNAM) SAF -
CLASSES=APPCLASS NODB EXIT=KLVSFPTX

c) If the parameters for member KLVINNAM are not configured in one of the ways specified in (b) above, this is a FINDING.

Fix Text: The Systems Programmer and IAO will ensure that the parameter options for member KLVINNAM are coded to the below specifications.

Review the member KLVINNAM in the TLVPARM DD statement concatenation of the CL/SuperSession STC procedure. (This member is located in SYS3.OMEGAMON.qualifier.RLSPARM.) Ensure all session manager security parameters and control options are in compliance according to the following:

DEFAULT DSNAME(SYS3.OMEGAMON.qualifier.RLSNAM) RACF -
NODB CLASSES=APPCLASS

CCI: CCI-000035

Group ID (Vulid): V-224469
Group Title: ZB000043
Rule ID: SV-27260r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCLSR043
Rule Title: CL/SuperSession APPCLASS member is not configured in accordance with the proper security requirements.

Vulnerability Discussion: Product configuration/parameters control the security and operational characteristics of products. If these parameter values are improperly specified, security and operational controls may be weakened. This exposure may threaten the availability of the product applications, and compromise the confidentiality of customer data.

IAControls: ECCD-1, ECCD-2

Check Content:

a) Review the member APPCLASS in SYS3.OMEGAMON.qualifier.RLSPARM of the RLSPARM initialization parameter library.

b) If the parameters for the member APPCLASS are configured as follows, there is

NO FINDING:

VGWAPLST EXTERNAL=APPL

c) If the parameters for the member APPCLASS are not configured as specified in

(b) above, this is a FINDING.

Reference: OS/390 STIG 6.2.2 (6)

Fix Text: The Systems Programmer and IAO will ensure that the parameter options for member APPCLASS are coded to the below specifications.

Review the member APPCLASS in the TLVPARM DD statement concatenation of the

CL/SuperSession STC procedure. (This member is located in SYS3.OMEGAMON.qualifier.RLSPARM.) Ensure all session manager security parameters

and control options are in compliance according to the following:

VGWAPLST EXTERNAL=APPL

CCI: CCI-000035

UNCLASSIFIED