

VANGUARD

Integrity Professionals, Inc.

Enterprise Security Software

z/OS CL/SuperSession for ACF2 STIG

Version: 6

Release: 10

29 Dec 2020

Group ID (Vulid): V-18014
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/Superssion 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/Superssion 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/Superssion 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-22689

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-16932

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

- SENSITVE.RPT(KLSRPT)

Automated Analysis:

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

- PDI(ZCLS0000)

b) Verify that access to the CL/SuperSession Install data sets are properly restricted.

___ The ACF2 data set rules for the data sets does not restrict UPDATE and/or ALTER access to systems programming personnel.

___ The ACF2 data set rules for the data sets does not specify that all (i.e., failures and successes) UPDATE and/or ALTER 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: 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 have 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

SYS2.OMEGAMON.V-.TLSLOAD
SYS2.OMEGAMON.V-.TLVLOAD
SYS3.OMEGAMON
SYS3.OMEGAMON.RLSLOAD

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

\$KEY(SYS2)
OMEGAMON.- UID(syspauDt) R(A) W(L) A(L) E(A)
OMEGAMON.V-.TLSLOAD UID(syspauDt) R(A) W(L) A(L) E(A)
OMEGAMON.V-.TLVLOAD UID(syspauDt) R(A) W(L) A(L) E(A)
OMEGAMON.- UID(audtaudt) R(A) E(A)

\$KEY(SYS3)
OMEGAMON.- UID(syspauDt) R(A) W(L) A(L) E(A)
OMEGAMON.RLSLOAD UID(syspauDt) R(A) W(L) A(L) E(A)
OMEGAMON.- UID(audtaudt) R(A) E(A)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067
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:
Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITVE.RPT(KLSSTC)

Automated Analysis:

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

- PDI(ZCLS0001)

Verify that the accesses to the CL/SuperSession STC data sets are properly restricted. If the following guidance is true, this is not a finding.

___ The ACF2 data set access authorizations restrict READ access to auditors and authorized users.

___ The ACF2 data set access authorizations restrict WRITE and/or greater access to systems programming personnel.

___ The ACF2 data set rules for the data sets does not restrict WRITE and/or greater access to the product STC(s) and/or batch job(s).

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 dataset 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:

\$KEY(SYS3)
OMEGAMON.RLSNAF UID(*) R(A) E(A)
OMEGAMON.RLSNAF UID(audtaudt) R(A) E(A)

OMEGAMON.RLSNAF UID(syspau dt) R(A) W(A) A(A) E(A)
OMEGAMON.RLSNAF UID(stc KLS) R(A) W(A) A(A) E(A)
OMEGAMON.RLSNAM UID(*) R(A) E(A)
OMEGAMON.RLSNAM UID(audtaudt) R(A) E(A)
OMEGAMON.RLSNAM UID(syspau dt) R(A) W(A) A(A) E(A)
OMEGAMON.RLSNAM UID(stc KLS) R(A) W(A) A(A) E(A)
OMEGAMON.RLSTDB UID(*) R(A) E(A)
OMEGAMON.RLSTDB UID(audtaudt) R(A) E(A)
OMEGAMON.RLSTDB UID(syspau dt) R(A) W(A) A(A) E(A)
OMEGAMON.RLSTDB UID(stc KLS) R(A) W(A) A(A) E(A)
OMEGAMON.RLSVLOG UID(*) R(A) E(A)
OMEGAMON.RLSVLOG UID(audtaudt) R(A) E(A)
OMEGAMON.RLSVLOG UID(syspau dt) R(A) W(A) A(A) E(A)
OMEGAMON.RLSVLOG UID(stc KLS) R(A) W(A) A(A) E(A)

CCI: CCI-001499

Group ID (Vulid): V-17452

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

IACControls: ECCD-1, ECCD-2

Check Content:

a) Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ATTSTC)

b) If the logonid for the CL/SUPERSESSION started task includes MUSASS and NO-SMC, there is NO FINDING.

c) If the logonid for the CL/SUPERSESSION started task does not include MUSASS and/or NO-SMC, this is a FINDING.

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:

INSERT KLS NAME(STC, CL/SuperSession) MUSASS NO-SMC STC

CCI: CCI-000764

Group ID (Vulid): V-22690

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:

Review the member KLVINNAM in the TLV Parm DD statement concatenation of the CL/SuperSession STC procedure. (This member is located in SYS3.OMEGAMON.qualifier.RLS Parm.)

Automated Analysis

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

- PDI(ZCLS0042)

If one of the following configuration settings is specified, this is not a finding.

DEFAULT DSNAME(SYS3.OMEGAMON.qualifier.RLSNAM)

NORACF
CLASSES=APPCLASS
NODB
EXIT=KLSA2NEV

(The following is for z/OS CAC logon processing)
DEFAULT DSNAME(SYS3.OMEGAMON.qualifier.RLSNAM)
SAF
CLASSES=APPCLASS
NODB
EXIT=KLSSFPTX

Fix Text: Ensure that the parameter options for member KLVINNAM are coded to the below specifications.

(Note: The data set identified below is an example of a possible installation. The actual data set is determined when the product is actually installed on a system through the product's installation guide and can be site specific.)

Review the member KLVINNAM in the TLV Parm 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)
NORACF
CLASSES=APPCLASS
NODB
EXIT=KLSA2NEV

(The following is for z/OS CAC logon processing)
DEFAULT DSNAME(SYS3.OMEGAMON.qualifier.RLSNAM)
SAF
CLASSES=APPCLASS
NODB
EXIT=KLSSFPTX

CCI: CCI-000035

Group ID (Vulid): V-22691
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