VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

z/OS CL/SuperSession for TSS STIG

Version: 6

Release: 10

27 Apr 2018

XSL Release 1/29/2015 Sort by: STIGID

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.

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:

- To view the Common profile select: _Common
- To view the SUPERSESSION profile select: _SupSess

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

- PDI(ZCLS0040)

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.

Check Content:
a) Review the member KLVINNAF in the TLVPARM DD statement concatenation of the CL/Supersession STC procedure. (This member is located in SYS3.OMEGAMON.qualifier.RLSPARM.)

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

- EXAM.RPT(SMFOPTS)

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

- PDI(ZCLS0041)

b) If the SMF= field specifies an SMF record number, review the SMFOPTS report to verify SMF is writing that record type.

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.

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-27092r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZCLST000
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.

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

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

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 are an example of data sets to be protected:
sys2.omegamon.
sys2.omegamon.*.tlsload
sys2.omegamon.*.tlvload
sys3.omegamon.
sys3.omegamon.rlsload

The following commands are provided as an example for implementing dataset controls:
TSS PERMIT(syspaudt) DSN(sys2.omegamon.) ACCESS(r)
TSS PERMIT(syspaudt) DSN(sys2.omegamon.) ACCESS(all) ACTION(audit)
TSS PERMIT(syspaudt) DSN(sys2.omegamon.*.tlsload) ACCESS(r)
TSS PERMIT(syspaudt) DSN(sys2.omegamon.*.tlsload) ACCESS(all) ACTION(audit)
TSS PERMIT(syspaudt) DSN(sys2.omegamon.*.tlvload) ACCESS(r)
TSS PERMIT(syspaudt) DSN(sys2.omegamon.*.tlvload) ACCESS(all) ACTION(audit)
TSS PERMIT(syspaudt) DSN(sys3.omegamon.) ACCESS(r)
TSS PERMIT(syspaudt) DSN(sys3.omegamon.) ACCESS(all) ACTION(audit)
TSS PERMIT(syspaudt) DSN(sys3.omegamon.*.rlsload) ACCESS(r)

TSS PERMIT(syspaudt) DSN(sys3.omegamon.*.rlsload) ACCESS(all) ACTION(audit)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-27098r3_rule
Severity: CAT II
Rule Version (STIG-ID): ZCLST001
Rule Title: CL/SuperSession STC data sets must be 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.

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 TSS data set access authorizations restrict READ access to auditors and authorized users.

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

___ The TSS 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 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:

TSS PERMIT(syspaudt) DSN(sys3.omegamon.rlsnaf) ACCESS(ALL)
TSS PERMIT(kls) DSN(sys3.omegamon.rlsnaf) ACCESS(ALL)
TSS PERMIT(audtaudt) DSN(sys3.omegamon.rlsnaf) ACCESS(READ)
TSS PERMIT(all) DSN(sys3.omegamon.rlsnaf) ACCESS(READ)

TSS PERMIT(syspaudt) DSN(sys3.omegamon.rlsnam) ACCESS(ALL)
TSS PERMIT(kls) DSN(sys3.omegamon.rlsnam) ACCESS(ALL)
TSS PERMIT(audtaudt) DSN(sys3.omegamon.rlsnam) ACCESS(READ)
TSS PERMIT(all) DSN(sys3.omegamon.rlsnam) ACCESS(READ)

TSS PERMIT(syspaudt) DSN(sys3.omegamon.rlstdb) ACCESS(ALL)
TSS PERMIT(kls) DSN(sys3.omegamon.rlstdb) ACCESS(ALL)
TSS PERMIT(audtaudt) DSN(sys3.omegamon.rlstdb) ACCESS(READ)
TSS PERMIT(all) DSN(sys3.omegamon.rlstdb) ACCESS(READ)

TSS PERMIT(syspaudt) DSN(sys3.omegamon.rlsvlog) ACCESS(ALL)
TSS PERMIT(kls) DSN(sys3.omegamon.rlsvlog) ACCESS(ALL)
TSS PERMIT(audtaudt) DSN(sys3.omegamon.rlsvlog) ACCESS(READ)
TSS PERMIT(all) DSN(sys3.omegamon.rlsvlog) ACCESS(READ)

CCI: CCI-001499

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-28592r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCLST030
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.

Check Content:
a) Refer to the following reports produced by the TSS Data Collection:

- TSSCMDS.RPT(@ACIDS)

b) Review the CL/SuperSession STC/Batch ACID(s) for the following:

___ Is defined as KLS for the ACID.

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

___ Is defined with Master Facility of KLS.

___ Is sourced to the INTRDR.

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

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

Fix Text: The Systems Programmer and IAO will ensure that the started task for 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:

TSS CRE(KLS) DEPT(Dept) NAME('CL/SuperSession STC') -
FAC(STC) MASTFAC(KLS) PASSWORD(password,0) -
SOURCE(INTRDR)

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-27238r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCLST032
Rule Title: CL/SuperSession Started task(s) must be properly defined to the Started Task Table ACID for Top Secret.

Vulnerability Discussion: Access to product resources should be restricted to only those individuals responsible for the application connectivity and who have a requirement to access these resources. Improper control of product resources could potentially compromise the operating system, ACP, and customer data.

Check Content:
Refer to the following report produced by the TSS Data Collection:

- TSSCMDS.RPT(#STC)

Automated Analysis
Refer to the following report produced by the TSS Data Collection:

- PDI(ZCLS0032)

Verify that the CL/SuperSession started task(s) is (are) defined in the TSS STC record.

Fix Text: The CL/SuperSession system programmer and the IAO will ensure that a product's started task(s) is (are) properly identified and/or defined to the System ACP.

A unique ACID must be assigned for the CL/SuperSession started task(s) thru a corresponding STC table entry.

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

TSS ADD(STC) PROCNAME(KLS) ACID(KLS)

CCI: CCI-000764

Group ID (Vulid): V-17469
Group Title: ZB000036
Rule ID: SV-27240r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCLST036
Rule Title: CL/SuperSession is not properly defined to the Facility Matrix Table for Top Secret.

Vulnerability Discussion: Improperly defined security controls for the Product could result in the compromise of the network, operating system, and customer data.

Check Content:
a) Refer to the following report produced by the TSS Data Collection:

- TSSCMDS.RPT(FACLIST) - Preferred report containing all control option values in effect including default values
- TSSCMDS.RPT(TSSPRMFL) - Alternate report containing only control option values explicitly coded at TSS startup

b) If KLS is properly defined in the Facility Matrix table, there is NO FINDING:

c) If KLS is improperly defined in the Facility Matrix table, this is a FINDING.

Fix Text: Define the CT/Engine started task name KLS as a Facility to TOP SECRET in the Facility Matrix Table using the following example:

*KLS CL/SUPERSESSION
FACILITY(USERxx=NAME=KLS)
FACILITY(KLS=MODE=FAIL,ACTIVE,SHRPRF)
FACILITY(KLS=PGM=KLV,NOASUBM,NOABEND,NOXDEF)
FACILITY(KLS=ID=xx,MULTIUSER,RES,LUMSG,STMSG,WARNPW,SIGN(M))
FACILITY(KLS=NOINSTDATA,NORNDPW,AUTHINIT,NOPROMPT,NOAUDIT)
FACILITY(KLS=NOTSOC,LOG(INIT,SMF,MSG,SEC9))

CCI: CCI-000764

Group ID (Vulid): V-18011
Group Title: ZB000038
Rule ID: SV-27190r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCLST038

Rule Title: CL/SuperSession's Resouce 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.

Check Content:
a) Refer to the following report produced by the TSS Data Collection:

- TSSCMDS.RPT(#RDT)

b) If the resource class of KLS is defined, there is NO FINDING.

c) If the resource class of KLS is not defined, this is a FINDING.

Fix Text: Add the resource KLS to the TOP SECRET RDT using the following TSS command example:

TSS ADD(RDT) RESCLASS(KLS) RESCODE(xx)

(where xx is an unused hex value)

CCI: CCI-000336

CCI: CCI-002358

Group ID (Vulid): V-22690
Group Title: ZB000042
Rule ID: SV-27258r4_rule
Severity: CAT II
Rule Version (STIG-ID): ZCLST042
Rule Title: CL/SuperSession KLVINNAM member must be configured in accordance to security requirements.

Vulnerability Discussion: CL/SuperSession 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.

Check Content:
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.)

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) –
RACF –
CLASSES=APPCLASS –
NODB –
EXIT=KLSTSNEV

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

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 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 –
CLASSES=APPCLASS –
NODB –
EXIT=KLSTSNEV

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

EXIT=KLSNFPTX or KLSTSPTX

CCI: CCI-000035

Group ID (Vulid): V-22691
Group Title: ZB000043
Rule ID: SV-27261r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCLST043
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.

Check Content:
a) 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.)

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

- PDI(ZCLS0043)

b) If the parameters for the member APPCLASS are configured as follows, there is NO FINDING:

VGWAPLST EXTERNAL=KLS

c) If the parameters for the member APPCLASS are not configured as specified in (b) above, this is a FINDING.

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=KLS

CCI: CCI-000035

UNCLASSIFIED