

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

z/OS CSSMTP for RACF STIG

Version: 6

Release: 6

30 June 2023

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

Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-89725r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZSMTR001
Rule Title: IBM Communications Server Simple Mail Transfer Protocol
(CSSMTP) STC
data sets must be properly protected.

Vulnerability Discussion: IBM Communications Server Simple Mail Transfer Protocol (CSSMTP) STC data sets have the ability to use privileged functions and/or have access to sensitive data. Failure to properly restrict access to

their data sets could result in violating the integrity of the base product which could result in compromising the operating system or sensitive data.

Responsibility: Information Assurance Officer
IACcontrols: DCSL-1, ECAR-1, ECAR-2, ECAR-3, ECCD-1,

Check Content:

a) The following steps are necessary for reviewing the CSSMPToptions:

1. Request on-line access from the site administrator to view CSSMPT parameter settings.
2. Once access to the CSSMPT 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 CSSMPT profile select: _SupSess

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

c) If all options as specified in the Required CSSMPT Common Profile Options and Required CSSMPT 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 CSSMPT 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:

Ensure that WRITE and/or greater access to the IBM Communications Server Simple Mail Transfer Protocol (CSSMTP) STC data sets are limited to system programmers and CSSMTP STC and/or batch jobs only. READ access can be given to auditors at the ISSOs discretion.

The installing Systems Programmer will identify and document the product data sets and categorize them according to who will have what type of access and if required which type of access is logged. The installing systems programmer will identify any additional groups requiring access to specific data sets, and once documented the installing systems programmer 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 commands are provided as an example for implementing data set controls:

```
ad 'sys3. cssmtp.**' uacc(none) owner(sys3) -
audit(failures(read)) -
data('CSSMTP Output Data')
pe 'sys*.cssmtp.**' id(syspautd) acc(a)
pe 'sys*. cssmtp.**' id(tstcaudt) acc(a)
pe 'sys*. cssmtp.**' id(smptstc) acc(a)
pe 'sys*. cssmtp.**' id(audtaudt) acc(r)
```

CCI: CCI-001499

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-37480r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZSMTR030
Rule Title: IBM CSSMTP Started Task name is not properly identified and/or defined to the system ACP.

Vulnerability Discussion: IBM CSSMTP 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) Use Vanguards Analyzer product to look at the Started Procedures Analysis report: Do the following for the IBM CSSMTP started task, likely called CSSMTP.

- a. From Analyzer main Menu, go to 3;4; Press ENTER
- b. Key in SORT PROCNAME; Press ENTER
- c. Key in L CSSMTP; Press ENTER
- d. If the stc name is not found then IBM CSSMTP is not defined to RACF as a STC user.
- e. If found but has a R in the M column, review the message and ensure that the following does not appear: VSA346R The user ID does not have the protected attribute. If message exists, then user does not have the PROTECTED attribute. This is a finding.
- f. If found then you would use the U line command to determine if the userid is defined to RACF.
- g. Key the U line command for the IBM CSSMTP entry; Press ENTER
- h. 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 IBM CSSMTP started task is defined to the security database with the PROTECTED attribute, there is NO FINDING.

c) If the userid for the IBM CSSMTP started task is not defined to the security database or does not have the PROTECTED attribute, this is a FINDING.

Fix Text: The IBM CSSMTP system programmer and the IAO will ensure that a product's Started Task(s) is properly identified and/or defined to the System ACP.

If the product requires a Started Task, verify that it is properly defined to the System ACP with the proper attributes.

Most installation manuals will indicate how the Started Task is identified and any additional attributes that must be specified.

A sample is provided here:

```
au CSSMTP name('IBM CSSMTP') owner(stc) dfltgrp(stc) nopass
```

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-37483r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZSMTR032
Rule Title: IBM CSSMTP 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

IACControls: ECCD-1, ECCD-2

Check Content:

a) Use Vanguard's Analyzer product to look at the Started Procedures Analysis report: Look for the IBM CSSMTP started task. The name of the started task is likely CSSMTP.

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

b) If a STARTED resource class profile exists for the started task IBM CSSMTP, there is NO FINDING.

c) If neither a STARTED resource class profile or an ICHRIN03 entry exists for the started task for IBM CSSMTP, this is a FINDING.

Fix Text: The IBM CSSMTP system programmer and the IAO will ensure that a product's Started Task(s) is properly identified and/or defined to the System ACP.

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

A sample set of commands is shown here:

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

CCI: CCI-000764

UNCLASSIFIED