

VANGUARD

Integrity Professionals, Inc.

Enterprise Security Software

z/OS CSSMTP for ACF2 STIG

Version: 6

Release: 5

29 Dec 2020

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:

Examine the running started task for CSSMTP.

Verify that access to the IBM Communications Server Simple Mail Transfer Protocol (CSSMTP) STC data sets are properly restricted. The data sets to be protected are identified in the data set referenced in the DD statements of the CSSMTP started task(s) and/or batch job(s).

Alternately:

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

- SENSITVE.RPT(SMTPSTC)

Automated Analysis:

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

- PDI(ZSMT0001)

If the following guidance is true, this is not a finding.

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

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

___ The ACF2 data set access authorizations 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 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:

```
$KEY(SYS3)
TCPIP.CSSMTP.- UID(syspautd) R(A) W(A) A(A) E(A)
TCPIP.CSSMTP.- UID(tstcaudt) R(A) W(A) A(A) E(A)
TCPIP.CSSMTP.- UID(icststc) R(A) W(A) A(A) E(A)
TCPIP.CSSMTP.- UID(audtaudt) R(A) E(A)
```

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
IAControls: ECCD-1, ECCD-2

Check Content:
Refer to the following report produced by the ACF2 Data Collection:

- ACF2CMDS.RPT(ATTSTC)

Insure that the logonids(s) for the IBM CSSMTP started task(s) includes the following:

STC
NO-SMC

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.

Example:

SET LID
INSERT CSSMTP STC NO-SMC

CCI: CCI-000764

UNCLASSIFIED