VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

# z/OS CSSMTP for TSS STIG

Version: 6

Release: 5

27 Oct 2017

XSL Release 1/29/2015 Sort by: STIGID

---

Group ID (Vulid):  V-17067
Group Title:  ZB000001
Rule ID:  SV-89727r2_rule
Severity: CAT II
Rule Version (STIG-ID):  ZSMTT001
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.

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).
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 TSS data set access authorizations restrict READ access to auditors.

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

___ The TSS 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:

```
TSS PERMIT(audtaudt) DSN(SYS3.TCPIP.CSSMTP.) ACCESS(R)
TSS PERMIT(syspaudt) DSN(SYS3.TCPIP.CSSMTP.) ACCESS(R)
TSS PERMIT(tstcaudt) DSN(SYS3.TCPIP.CSSMTP.) ACCESS(R)
TSS PERMIT(icststc) DSN(SYS3.TCPIP.CSSMTP.) ACCESS(R)
TSS PERMIT(syspaudt) DSN(SYS3.TCPIP.CSSMTP.) ACCESS(ALL)
TSS PERMIT(tstcaudt) DSN(SYS3.TCPIP.CSSMTP.) ACCESS(ALL)
TSS PERMIT(icststc) DSN(SYS3.TCPIP.CSSMTP.) ACCESS(ALL)
```

CCI: CCI-001499

---

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-37481r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZSMTT030
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.

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

- TSSCMDS.RPT(@ACIDS)

Review each IBM CSSMTP STC/Batch ACID(s) for the following:

___ Defined with Facility of STC (the TSS FACILITY Matrix Table entry defined for this product), and/or BATCH for CSSMTP.

___ Is sourced to the INTRDR.

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:

```
TSS CREATE(CSSMTP) TYPE(USER) -
    NAME('IBM CSSMTP') DEPT(xxxx) -
   FAC(STC) -
   PASS(xxxxxxxx,0) -
   SOURCE(INTRDR) NOSUSPEND
```

CCI: CCI-000764

---

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-37484r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZSMTT032
Rule Title: IBM CSSMTP 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(ZSMT0032)

Verify that the IBM CSSMTP started task(s) is (are) defined in the TSS STC record.

Fix Text: The IBM CSSMTP 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 IBM CSSMTP 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(CSSMTP) ACID(CSSMTP)
```

CCI: CCI-000764

---