VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

z/OS CA 1 Tape Management for TSS STIG

Version: 6

Release: 8

25 Oct 2019

XSL Release 1/29/2015 Sort by: STIGID

Group ID (Vulid): V-22689
Group Title: ZB000041
Rule ID: SV-40107r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCA10041
Rule Title: CA 1 Tape Management system password will be changed from the default.

Vulnerability Discussion: CA 1 Tape Management default system password is common with all CA 1 systems. With this password, CA 1 tape processing can be deactivated. This could allow for unauthorized access to information stored on tape volumes and the CA 1 Tape Management Catalog (TMC). The result may threaten the integrity and availability of the CA 1 Tape Management System, and compromise the confidentiality of customer data.

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

- CA1RPT(TMSTMVT) – for r11.5 and below
- CA1RPT(TMOOPTxx) – for r12.0 and above

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

- PDI(ZCA10041)

For r11.5 and below refer to offset x'18' from the beginning of module TMSTMVT. For r12.0 and above refer to the SHUTDWN option specified in the TMOOPTxx. The TMOOPTxx member is specified in the TMOSYSxx member in the data set allocated by the TMSPARM DD statement in the TMSINIT STC. If the default CA 1 system password is not being utilized, this is not a finding.

NOTE: The default system password for CA 1 provided by CA is CA1(TMS). The default system passwords provided by SSO are SSOCA1DF and SSOC@1DF.

Fix Text: The systems programmer/IAO will ensure that the CA 1 system password is changed from the vendor default system password.

Verify upon installation that the password is not the same as the default password and user distributed with the original installation default.

For r11.5 and below refer to offset x'18' from the beginning of module TMSTMVT.

For r12.0 and above refer to the SHUTDWN option specified in the TMOOPTxx. The TMOOPTxx member is specified in the TMOSYSxx member in the data set allocated by

the TMSPARM DD statement in the TMSINIT STC.

NOTE: The default system password for CA 1 provided by CA is CA1(TMS). The default system passwords provided by SSO are SSOCA1DF and SSOC@1DF.

CCI: CCI-000035

Group ID (Vulid): V-17985
Group Title: ZB000060
Rule ID: SV-40108r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZCA10060
Rule Title: CA 1 Tape Management user exits, when in use, must be reviewed and/or approved.

Vulnerability Discussion: CA-1 Tape Management user exits, TMSUXnA and TMSUXnS, provide the capability to bypass or modify existing ACP controls. A review and evaluation of exit code must be performed to ensure that the integrity of the CA-1 processing environment is kept intact. Unauthorized usage of these exits may compromise the confidentiality and integrity of customer data.

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

- CA1RPT(TMSCKLVL)

Determine if CA 1 user exits, TMSUXnA and TMSUXnS (for r11.5 and below) or TMSXITA and TMSXITS (for r12.0 and above) are active.

If both CA 1 user exits are not found, this is not a finding.

If one or both user exits are installed and the following requirements are true, this is not a finding:

___ The usage and function of the user exit(s) is fully documented.
___ The use of the user exit(s) is approved.
___ All associated documentation is on file with the ISSO.

Fix Text: Ensure that the site ISSO has reviewed, evaluated, and approved the usage of CA 1 user exits, TMSUXnA and TMSUXnS (for r11.5 and below) or TMSXITA and TMSXITS (for r12.0 and above). If one or both user exits are installed and the following requirements will be followed:

The usage and function of the user exit(s) is fully documented.

The use of the user exit(s) is approved.

All associated documentation is on file with the ISSO.

CCI: CCI-000035

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-40069r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZCA1T000
Rule Title: CA 1 Tape Management installation data sets must be properly protected.

Vulnerability Discussion: CA 1 Tape Management installation data sets have the ability to use privileged functions and/or have access to sensitive data. Failure to properly restrict access to these 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(CA1PROD)

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

- PDI(ZCA10000)

Verify that the accesses to the CA 1 Tape Management installation data sets are properly restricted. If the following guidance is true, this is not a finding.

___ The TSS data set rules for the data sets restricts READ access to all authorized users.

___ The TSS data set rules for the data sets restricts WRITE and/or greater access to systems programming personnel.

___ The TSS data set rules for the data sets specify that all (i.e., failures

and successes) WRITE and/or greater access is logged.

Fix Text: Ensure that WRITE and/or greater access to CA 1 Tape Management installation data sets is limited to System Programmers only, and all WRITE and/or greater access is logged. READ access can be given to all 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 IAO to see that they are properly restricted to the ACP (Access Control Program) active on the system.

The following is an example of the type of data sets to be protected:
SYS2.CA1.
SYS2A.CA1.*.CAILIB
SYS2A.CA1.*.CAILPA
Or
SYS2A.CA1.*.CTAPLINK
SYS3.CA1.
SYS3A.CA1.*.CAILIB
Or
SYS3A.CA1.*.CTAPLINK
SYS3A.CA1.*.CTAPLPA

The following commands are provided as a sample for implementing data set controls:

TSS ADD(SYS2) DSN(SYS2)
TSS ADD(SYS2A) DSN(SYS2A)
TSS ADD(SYS3) DSN(SYS3)
TSS ADD(SYS3A) DSN(SYS3A)
TSS PERMIT(syspaudt) DSN(SYS2.CA1.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(syspaudt) DSN(SYS2.CA1.) ACCESS(READ)
TSS PERMIT(authorized users/ALL) DSN(SYS2.CA1.) ACCESS(READ)
TSS PERMIT(syspaudt) DSN(SYS2A.CA1.V*.CAILIB) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(syspaudt) DSN(SYS2A.CA1.V*.CAILIB) ACCESS(READ)
TSS PERMIT(authorized users/ALL) DSN(SYS2A.CA1.V*.CAILIB) ACCESS(READ)
TSS PERMIT(syspaudt) DSN(SYS2A.CA1.V*.CAILPA) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(syspaudt) DSN(SYS2A.CA1.V*.CAILPA) ACCESS(READ)
TSS PERMIT(authorized users/ALL) DSN(SYS2A.CA1.V*.CAILPA) ACCESS(READ)
Or
TSS PERMIT(syspaudt) DSN(SYS2A.CA1.V*.CTAPLINK) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(syspaudt) DSN(SYS2A.CA1.V*.CTAPLINK) ACCESS(READ)
TSS PERMIT(authorized users/ALL) DSN(SYS2A.CA1.V*.CTAPLINK) ACCESS(READ)
TSS PERMIT(syspaudt) DSN(SYS3.CA1.) ACCESS(ALL) ACTION(AUDIT)

TSS PERMIT(syspaudt) DSN(SYS3.CA1.) ACCESS(READ)
TSS PERMIT(authorized users/ALL) DSN(SYS3.CA1.) ACCESS(READ)
TSS PERMIT(syspaudt) DSN(SYS3A.CA1.V*.CAILIB) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(syspaudt) DSN(SYS3A.CA1.V*.CAILIB) ACCESS(READ)
TSS PERMIT(authorized users/ALL) DSN(SYS3A.CA1.V*.CAILIB) ACCESS(READ)
Or
TSS PERMIT(syspaudt) DSN(SYS3A.CA1.V*.CTAPLINK) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(syspaudt) DSN(SYS3A.CA1.V*.CTAPLINK) ACCESS(READ)
TSS PERMIT(authorized users/ALL) DSN(SYS3A.CA1.V*.CTAPLINK) ACCESS(READ)
TSS PERMIT(syspaudt) DSN(SYS3A.CA1.V*.CTAPLPA) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(syspaudt) DSN(SYS3A.CA1.V*.CTAPLPA) ACCESS(READ)
TSS PERMIT(authorized users/ALL) DSN(SYS3A.CA1.V*.CTAPLPA) ACCESS(READ)

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17067
Group Title: ZB000001
Rule ID: SV-87415r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCA1T001
Rule Title: CA-1 Tape Management STC data sets must be properly protected.

Vulnerability Discussion: CA-1 Tape Management STC data sets have the ability to use privileged functions and/or have access to sensitive data. Failure to properly restrict access to these 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 TSS Data Collection and Data Set and Resource Data Collection:

- SENSITVE.RPT(CA1STC)

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

- PDI(ZCA10001)

Verify that the accesses to CA1 Tape Management Started Tasks (STCs) 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.

___ 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 CA1 Tape Management STCs and/or batch users.

Fix Text: Ensure that WRITE and/or greater access to CA1 Tape management STC data sets is limited to System Programmers and/or CA1 Tape management STC(s) and/or batch user(s) only. READ access can be given to auditors.
(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.)

Data sets to be protected will be:
CA1.TMS* (Data sets that are altered by the product's STCs, this can be more specific.)

The following commands are provided as a sample for implementing data set controls:

TSS PERMIT(<syspaudt>) DSN(SYS3.CA1.TMS*.**) ACCESS(ALL)
TSS PERMIT(<Tape Management STCs and/or batch users >) DSN(SYS3.CA1.TMS*.**) ACCESS(ALL)
TSS PERMIT(<audtaudt >) DSN(SYS3.CA1.TMS*.**)

CCI: CCI-001499

Group ID (Vulid): V-17072
Group Title: ZB000003
Rule ID: SV-40072r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZCA1T003
Rule Title: CA 1 Tape Management TMC, AUDIT and optional RDS and VPD data sets will be properly protected.

Vulnerability Discussion: CA 1 Tape Management TMC and AUDIT and optional data

sets control the operations and access to the tape management system, and site specific information regarding tape volumes. Unauthorized access to these data sets could threaten the integrity and availability of the CA 1 Tape Management System, and compromise the confidentiality of customer data.

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

- SENSITVE.RPT(CA1RPT)

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

- PDI(ZCA10003)

Ensure that all CA 1 Tape Management TMC, AUDIT and optional RDS and VPD data sets are properly protected. If the following guidance is true, this is not a finding.

___ The TSS data set access authorizations restricts READ access to application support personnel, production control and scheduling personnel, operations personnel, and auditors.

___ The TSS data set access authorizations restricts WRITE and/or greater access to only systems programming personnel and tape management personnel.

___ The TSS data set access authorizations restricts UPDATE access is limited to CA 1 batch production jobs, and CA 1 started tasks.

___ The TSS data set access authorizations specify that all (i.e., failures and successes) ALL access is logged.

Fix Text: The IAO will ensure that WRITE and/or greater access to CA 1 TMC, AUDIT and optional RDS and VPD data sets are limited to only systems programming personnel and tape management personnel. UPDATE access can be given to CA 1 STCs and/or batch users. READ access can be given to application support personnel, production control and scheduling personnel, operations personnel, and auditors. ALL access will be 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 and/or alter access for specific data sets, and once documented he will work with the IAO 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.)

Due to the unique file structure of the TMC and Audit data sets, CA 1 uses the YSVC programs to handle all direct I/O activity. Because standard OPEN/CLOSE macros are not used, typical data set security checks are not performed. Even if a user does not have read authority to these data sets, the YSVC programs can enable that user to read and update records within these files. Therefore, control READ access to the TMC and Audit data sets by the YSVCUNCD and YSVCCOND resource names. Typical users should be restricted to conditional READ access.

Restrict CA 1 batch production jobs, and CA 1 started tasks to the following access authority: Unconditional READ and UPDATE access to the TMC, Audit, Retention, and Vault Pattern Description data sets. NOTE: READ and UPDATE access to the TMC and Audit data sets are controlled by the YSVCUNCD and YSVCCOND resource names, and by standard ACP data set controls, because some CA 1 utilities use conventional OPEN/CLOSE methods.

The following commands are provided as a sample for implementing data set controls:

TSS ADD(SYS3) DSN(SYS3)
TSS PERMIT(<audtaudt>) DSN(SYS3.CA1.AUDIT) ACCESS(READ)
TSS PERMIT(<operaudt>) DSN(SYS3.CA1.AUDIT) ACCESS(READ)
TSS PERMIT(<pcspaudt>) DSN(SYS3.CA1.AUDIT) ACCESS(READ)
TSS PERMIT(CA1 STCs) DSN(SYS3.CA1.AUDIT) ACCESS(UPDATE)
TSS PERMIT(<syspaudt>) DSN(SYS3.CA1.AUDIT) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<syspaudt>) DSN(SYS3.CA1.AUDIT) ACCESS(UPDATE)
TSS PERMIT(<tapeaudt>) DSN(SYS3.CA1.AUDIT) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<tapeaudt>) DSN(SYS3.CA1.AUDIT) ACCESS(UPDATE)
TSS PERMIT(<tstcaudt>) DSN(SYS3.CA1.AUDIT) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<tstcaudt>) DSN(SYS3.CA1.AUDIT) ACCESS(UPDATE)
TSS PERMIT(<syspaudt>) DSN(SYS3.CA1.RDS) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<syspaudt>) DSN(SYS3.CA1.RDS) ACCESS(UPDATE)
TSS PERMIT(<tapeaudt>) DSN(SYS3.CA1.RDS) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<tapeaudt>) DSN(SYS3.CA1.RDS) ACCESS(UPDATE)
TSS PERMIT(<tstcaudt>) DSN(SYS3.CA1.RDS) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<tstcaudt>) DSN(SYS3.CA1.RDS) ACCESS(UPDATE)
TSS PERMIT(<audtaudt>) DSN(SYS3.CA1.TMC) ACCESS(READ)
TSS PERMIT(<operaudt>) DSN(SYS3.CA1.TMC) ACCESS(READ)
TSS PERMIT(<pcspaudt>) DSN(SYS3.CA1.TMC) ACCESS(READ)
TSS PERMIT(CA1 STCs) DSN(SYS3.CA1.TMC) ACCESS(UPDATE)
TSS PERMIT(<syspaudt>) DSN(SYS3.CA1.TMC) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<syspaudt>) DSN(SYS3.CA1.TMC) ACCESS(UPDATE)
TSS PERMIT(<tapeaudt>) DSN(SYS3.CA1.TMC) ACCESS(ALL) ACTION(AUDIT)

TSS PERMIT(<tapeaudt>) DSN(SYS3.CA1.TMC) ACCESS(UPDATE)
TSS PERMIT(<tstcaudt>) DSN(SYS3.CA1.TMC) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<tstcaudt>) DSN(SYS3.CA1.TMC) ACCESS(UPDATE)
TSS PERMIT(<syspaudt>) DSN(SYS3.CA1.VPD) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<syspaudt>) DSN(SYS3.CA1.VPD) ACCESS(UPDATE)
TSS PERMIT(<tapeaudt>) DSN(SYS3.CA1.VPD) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<tapeaudt>) DSN(SYS3.CA1.VPD) ACCESS(UPDATE)
TSS PERMIT(<tstcaudt>) DSN(SYS3.CA1.VPD) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<tstcaudt>) DSN(SYS3.CA1.VPD) ACCESS(UPDATE)

CCI: CCI-000035

Group ID (Vulid): V-17947
Group Title: ZB000020
Rule ID: SV-40075r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCA1T020
Rule Title: CA 1 Tape Management command resources will be properly defined and protected.

Vulnerability Discussion: CA 1 Tape Management can run with sensitive system privileges, and potentially can circumvent system controls. Failure to properly control access to product resources could result in the compromise of the operating system environment, and compromise the confidentiality of customer data. Many utilities assign resource controls that can be granted to system programmers only in greater than read authority. Resources are also granted to certain non systems personnel with read only authority.

On-line applications offer the capabilities to directly access the CA 1 Tape Management Catalog (TMC) for query and update purposes. CA 1 special tape handling privileges offer the ability to process special tape requirements, such as BLP and foreign tapes. Uncontrolled access to these CA 1 features and facilities may threaten the integrity and availability of the CA 1 tape management system, and compromise the confidentiality of customer data.

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

- TSSCMDS.RPT(WHOOCA1C)
- SENSITVE.RPT(WHOHCA1C)

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

- PDI(ZCA10020)

Ensure that all CA 1 command resources are properly protected according to the requirements specified in CA 1 Command Resources table in the z/OS STIG Addendum. If the following guidance is true, this is not a finding.

___ The TSS resources and/or generic equivalent as designated in the above table are owned or DEFPROT is specified for the resource class.

___ The TSS resource access authorizations restrict access to the appropriate personnel as designated in the above table.

___ The TSS resource logging is specified as designated in the above table.

Fix Text: The IAO will work with the systems programmer to verify that the following are properly specified in the ACP.

Ensure that the CA 1 Tape Management command resource access is in accordance with those outlined in CA 1 Command Resources table in the zOS STIG Addendum.

Use CA 1 Command Resources and CA 1 Command Resource for TSS tables in the zOS STIG Addendum. These tables list the resources, access requirements, and the resource class for CA 1 Command Resources; ensure the following guidelines are followed:

The TSS resources and/or generic equivalent as designated in the above table are owned or DEFPROT is specified for the resource class.

The TSS resource access authorizations restrict access to the appropriate personnel as designated in the above table.

The TSS resource logging is specified as designated in the above table.

The following commands are provided as a sample for implementing resource controls:

TSS ADD(dept-acid) CACMD(L0DELETE)
TSS PERMIT(tapeaudt) CACMD(L0DELETE) ACCESS(READ)

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17982

Group Title: ZB000021
Rule ID: SV-40078r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZCA1T021
Rule Title: CA 1 Tape Management function and password resources will be properly defined and protected.

Vulnerability Discussion: CA 1 Tape Management can run with sensitive system privileges, and potentially can circumvent system controls. Failure to properly control access to product resources could result in the compromise of the operating system environment, and compromise the confidentiality of customer data. Many utilities assign resource controls that can be granted to system programmers only in greater than read authority. Resources are also granted to certain non systems personnel with read only authority.

CA 1 on-line applications offer the capabilities to directly access the CA 1 Tape Management Catalog (TMC) for query and update purposes. CA 1 special tape handling privileges offer the ability to process special tape requirements, such as BLP and foreign tapes. Uncontrolled access to these CA 1 features and facilities may threaten the integrity and availability of the CA 1 tape management system, and compromise the confidentiality of customer data.

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

- TSSCMDS.RPT(WHOOCA1T)
- SENSITVE.RPT(WHOHCA1T)

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

- CA1RPT(TMSSECAB)
- CA1RPT(TMSTMVT) – for r11.5 and below
- CA1RPT(TMOOPTxx) – for r12.0 and above
- CA1RPT(TMOSECxx) – for r12.6 and above

Automated Analysis requiring additional analysis
Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ZCA10021)

Ensure that all CA 1 function and password resources are properly protected according to the requirements specified in the CA 1 Function and Password Resources table in the z/OS STIG Addendum. If the following guidance is true, this is not a finding.

___ The TSS resources and/or generic equivalent as designated in the above table are owned and/or DEFPROT is specified for the resource class.

___ The TSS resource access authorizations restrict access to the appropriate personnel as designated in the above table.

___ The TSS resource logging is specified as designated in the above table.

Note: CA 1 password resources may require additional analysis to ensure access authorization is justified. CA 1 system password is obtained at offset x'18' from the beginning of module TMSTMVT for r11.5 and below and SHUTDWN option specified in the TMOOPTxx for r12.0 and above. CA 1 Online User Passwords can be obtained from TMSSECAB for all releases or TMOSECxx, if present, for r12.6 and above.

Fix Text: The IAO will work with the systems programmer to verify that the following are properly specified in the ACP.

Ensure that the CA 1 function and password resource access is in accordance with those outlined in CA 1 Function and Password Resources table in the zOS STIG Addendum.

Use CA 1 Function and Password Resources and CA 1 Function and Password Resources for TSS tables in the zOS STIG Addendum. These tables list the resources, access requirements, and the resource class for CA 1 Function and Password Resources; ensure the following guidelines are followed:

The TSS resources and/or generic equivalent as designated in the above table are owned or DEFPROT is specified for the resource class.

The TSS resource access authorizations restrict access to the appropriate personnel as designated in the above table.

The TSS resource logging is specified as designated in the above table.

The following commands are provided as a sample for implementing resource controls:

TSS ADD(dept-acid) CATAPE(BLPRES)
TSS PERMIT(tapeaudt) CATAPE(BLPRES) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(syspaudt) CATAPE(BLPRES) ACCESS(UPDATE) ACTION(AUDIT)

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17452
Group Title: ZB000030
Rule ID: SV-40081r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCA1T030
Rule Title: CA 1 Tape Management Started Task name will be properly identified and/or defined to the system ACP.

Vulnerability Discussion: CA 1 Tape Management 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)

Verify that the ACID(s) for the CA 1 Tape Management started task(s) is (are) properly defined. If the following attributes are defined, this is not a finding.

FACILITY(STC, BATCH)
PASSWORD(xxxxxxxx,0)
SOURCE(INTRDR)
NOSUSPEND
MASTFAC(CA1)

Fix Text: The IAO working with the systems programmer will ensure the CA 1 Tape Management 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.

The following commands are provided as a sample for defining Started Task(s):

```
TSS CREATE(TMSINIT) TYPE(USER) -
     NAME('STC, CA 1 Tape Management') DEPT(xxxx) -
```

```
    FAC(STC,BATCH) PASS(xxxxxxxx,0) -
    SOURCE(INTRDR) NOSUSPEND –
    MASTFAC(CA1)
TSS CREATE(CTS) TYPE(USER) -
     NAME('STC, CA 1 Common Tape System') DEPT(xxxx) -
    FAC(STC,BATCH) PASS(xxxxxxxx,0) -
    SOURCE(INTRDR) NOSUSPEND –
    MASTFAC(CA1)
```

CCI: CCI-000764

Group ID (Vulid): V-17454
Group Title: ZB000032
Rule ID: SV-40083r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCA1T032
Rule Title: CA 1 Tape Management Started task will 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(ZCA10032)

If the CA 1 Tape Management started task(s) is (are) defined in the TSS STC record, this is not a finding.

Fix Text: The IAO working with the systems programmer will ensure the CA 1 Tape Management Started Task(s) is properly identified and/or defined to the System ACP.

A unique ACID must be assigned for the CA 1 Tape Management started task(s) thru a corresponding STC table entry.

The following commands are provided as a sample for defining Started Task(s):

TSS ADD(STC) PROCNAME(TMSINIT) ACID(TMSINIT)
TSS ADD(STC) PROCNAME(CTS) ACID(CTS)

CCI: CCI-000764

Group ID (Vulid): V-17469
Group Title: ZB000036
Rule ID: SV-40631r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCA1T036
Rule Title: CA 1 Tape Management will be properly defined to the Facility Matrix Table.

Vulnerability Discussion: Improperly defined security controls for CA 1 Tape Management could result in the compromise of the network, operating system, and customer data.

Check Content:
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

If the CA 1 Tape Management Facility Matrix table is defined as stated below, this is not a finding.

FACILITY DISPLAY FOR CA1
INITPGM=TMS id=xx TYPE=099
ATTRIBUTES=IN-USE,ACTIVE,SHRPRF,NOASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=NOLUMSG,NOSTMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,NOWARNPW,NOTSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,NOEODINIT,IJU,NODORMPW,NONPWR
ATTRIBUTES=LUUPD
MODE=FAIL DOWN=GLOBAL LOGGING=INIT,SMF,MSG,SEC9
UIDACID=8 LOCKTIME=000 DEFACID=*NONE* KEY=8
MAXUSER=03000 PRFT=003

Fix Text: The IAO working with the systems programmer will ensure the Facility Matrix Table for CA 1 Tape Management is proper defined using the following example:

*****CA1

FAC(USERxx=NAME=CA1,PGM=TMS,ID=nn,ACTIVE,NOASUBM)
FAC(CA1=NOLUMSG,NOSTMSG,NORNDPW,NOWARNPW,MODE=FAIL)
FAC(CA1=LOG(SMF,INIT,MSG,SEC9),UIDACID=8,LOCKTIME=000)

CCI: CCI-000764

Group ID (Vulid): V-18014
Group Title: ZB000040
Rule ID: SV-40102r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZCA1T040
Rule Title: CA 1 Tape Management external security options must be specified properly.

Vulnerability Discussion: CA 1 Tape Management offers multiple external security interfaces that are controlled by parameters specified in TMOOPT00. These interfaces provide security controls for several CA 1 system and user functions. Without proper controls of these sensitive functions, the integrity of the CA 1 Tape Management System and the confidentiality of data stored on tape volumes may be compromised.

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

- CA1RPT(TMSSTATS)

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

- PDI(ZCA10040)

CA 1 external security utilizing TSS is accomplished in the manner described in this section.

NOTE: The TMOOPTxx member is specified in the TMOSYSxx member in the data set allocated by the TMSPARM DD statement in the TMSINIT STC. By default, the suffix 00 is used for these members. However, overrides can be specified by PARM value(s) on the EXEC statement in the TMSINIT STC and/or in the TMOSYSxx member.

Review the options and values of the below CA 1 parameters. If the options are set to the specified value, this is not a finding.

CA 1 SECURITY OPTIONS - TSS
Option Standard Value
BATCH YES obsolete as of r12.0

CATSEC YES obsolete as of r12.0
CMD YES
CREATE see Note 1
DSNB YES
FUNC YES see Note 2
OCEOV YES see Note 3
PMASK Do not specify or change
PSWD YES
SCRTCH NO
SECWTO YES
UNDEF FAIL
UX0AUPD NO see Note 4
YSVC YES

Note 1 The CREATE parameter defines the level of access that is required to create a data set on tape. The default value is UPDATE. However, the vendor recommends the value be set to CREATE if you are running CA Top Secret or ACF2 and ALTER if you are running RACF..

Note 2 The FUNC option provides supplementary security for BLP access. The tape label bypass privilege must still be specified in the ACP userid record to allow access to BLP processing.

Note 3 The data set OPEN/CLOSE security call will be handled by the CA 1 interface. To avoid duplication of security checking, the control option TAPE should be turned OFF in the TOP SECRET Control Options.

Note 4 The UX0AUPD will specify YES only if you alter the fields in the TMC and the TMSUXxA (for r11.5 and below) or TMSXITA (for r12.0 and above) is changed.

Fix Text: The systems programmer/IAO will ensure that the CA 1 external security options are specified in accordance with the ACP being used. CA 1 Tape Management ACP security interfaces are controlled by options coded in the TMOOPTxx member identified in the TMOSYSxx member of the data set allocated by the TMSPARM DD statement in the TMSINIT STC. The specific required option settings are dependent on the ACP in use on the system.

CA 1 SECURITY OPTIONS - TSS
OPTION STANDARD VALUE
BATCH YES obsolete as of r12.0
CATSEC YES obsolete as of r12.0
CMD YES
CREATE see note 1
DSNB YES
FUNC YES see note 2
OCEOV YES see note 3
PMASK Do not specify or change

PSWD YES
SCRTCH NO
SECWTO YES
UNDEF FAIL
UX0AUPD NO see note 4
YSVC YES

Note 1 The CREATE parameter defines the level of access that is required to create a data set on tape. The default value is UPDATE. However, the vendor recommends the value be set to CREATE if you are running CA Top Secret or ACF2 and ALTER if you are running RACF.

Note 2 The FUNC option provides supplementary security for BLP access. The tape label bypass privilege must still be specified in the ACP userid record to allow access to BLP processing.

Note 3 The data set OPEN/CLOSE security call will be handled by the CA 1 interface. To avoid duplication of security checking, the control option TAPE should be turned OFF in the TOP SECRET Control Options record.

Note 4 The UX0AUPD will specify YES only if you alter the fields in the TMC and the TMSUXxA (for r11.5 and below) or TMSXITA (for r12.0 and above) is changed.

CCI: CCI-000035
