

VANGUARD

Integrity Professionals, Inc.

Enterprise Security Software

z/OS CA 1 Tape Management for ACF2 STIG

Version: 6

Release: 7

29 Dec 2020

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.

Responsibility: Information Assurance Officer

IACControls: ECCD-1, ECCD-2

Check Content:

- a) Determine if the CA-1 default system password CA1(TMS) is being utilized.
- b) If the installed release of CA-1 is 11.5 or below do the following:
 - 1. From Analyzer Main Menu, go to 3;B Sensitive and Critical Datasets Analysis and place an S next to Authorized Program Facility (APF) Table, then ENTER.
 - 2. Locate the CA-1 LINKLIB dataset and enter an H in the Opt column for that dataset to search for a character string in the TMSTMVT module .
 - 3. On the next panel, enter TMSTMVT in the Member list field and

CCA1(TMS) in the Search text field.

4. If the Count column of the next display is zero (0), there is NO FINDING (meaning the default CA-1 system password is not being used).

5. If the Count column of the next display is not zero, there is a FINDING as the default CA-1 system password has been found.

c) If the installed release of CA-1 is 12.0 or above do the following:

1. Check the SHUTDOWN option for the presence of the CA_! default password.

2. To examine the SHUTDOWN option

a. Find the TMSINIT STC proc.

b. Find the TMSPARM DD statement which points to a PDS.

c. Look at the member TMOSYSxx in this dataset

d. Member TMOSYSxx will point to member TMOOPTxx which specifies the SHUTDOWN option.

e. If the CA_1 password is specified in the SHUTDOWN option, this is a FINDING.

f. If the CA_1 password is not specified in the SHUTDOWN option, there is no FINDING.

Note re c: above needs verification as to what data is actually present on the SHUTDOWN option statement and also clarification as to where member TMOOPTxx and TMOSYSxx actually are . Are they both PDS members and if so of which PDSs exactly?

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 SHUTDOWN 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-40108r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZCA10060

Rule Title: CA 1 Tape Management exits when in use will 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.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2, ECSD-1, ECSD-2

Check Content:

1. If the installed release of CA-1 is 11.5 or below do the following:
 - a) Determine if either of the CA-1 security exits TMSUXnA and/or TMSUXnS

is active.

b) From whatever tool is being used to view JES output, select any CA_1 startup JES spool output data.

1. Find all occurrences of TMSUX.
2. For any exit that indicates ACTIVATED, determine if the name of the exit matches the TMSUXnA or TMSUXnS security exit criteria.

c) If there is an active TMSUXnA or TMSUXnS security exit ensure that it meets the following requirements:

1. The usage and function of any active exit is fully documented,
2. The exit code has been reviewed by a qualified security analyst,
3. The use of the any active exit is approved by Security Management,
4. All associated documentation is filed in the appropriate location.

d) If all of the items in (c) above are satisfied, there is no FINDING.

e) If any of the items in (c) above are not satisfied, there is a FINDING.

2. If the installed release of CA-1 is 12.0 or above do steps 1.a to 1. e above, but
search for exit names TSMXITA and TSMXITS instead of TMSUXnA and TMSUXnS.

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

The usage and function of the exit(s) is fully documented.
DISA Field Security Operations reviewed the exit code.
The use of the exit(s) is approved by DISA Field Security Operations.
All associated documentation is on file with the IAO.

CCI: CCI-000035

Group ID (Vulid): V-16932
Group Title: ZCA1A000
Rule ID: SV-40068r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCA1A000
Rule Title: CA 1 Tape Management installation data sets will 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.

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

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 ACF2 data set rules for the data sets restricts READ access to all authorized users.

___ The ACF2 data set rules for the data sets restricts WRITE and/or greater access to systems programming personnel.

___ The ACF2 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 CA1 Tape management STC data sets is limited to System Programmers and/or CA1 Tape management STC(s) and/or batch user(s) only.

(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:

\$KEY(SYS3)

CA1.TMS*.**- UID(<syspau>) R(A) W(A) A(A) E(A)

CA1.TMS*.**- UID(<Tape Management STCs and/or batch users >) R(A) W(A) A(A) E(A)

CA1.TMS*.**- UID(<audtaudt>) R(A) E(A)

CCI: CCI-000213

CCI: CCI002234

Group ID (Vulid): V-17067

Group Title: ZB000001

Rule ID: SV-87411r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZCA1A001

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.

Responsibility: Information Assurance Officer

IACControls: DCSL-1, ECAR-1, ECAR-2, ECAR-3, ECCD-1

Check Content:

Refer to the following report produced by the 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 the CA CA-1 installation data sets are properly restricted.

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

___ The RACF data set rules for the data sets restricts UPDATE and/or ALTER access to systems programming personnel.

___ The RACF data set rules for the data sets specify that all (i.e., failures and successes) UPDATE and/or ALTER access are logged.

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.)

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 alter 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.

Data sets to be protected will be:

CAI.TMS.**

CAI.TMS.** (data sets that are not altered by product STCs, can be more specific)

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

```
ad 'CAI.TMS.**' uacc(none) owner(sys2) -  
    audit(success(update) failures(read)) -  
    data('CA CA-1 Install DS')  
pe 'CAI.TMS.**' id(<syspauDt> <tstcaudt>) acc(a)  
pe 'CAI.TMS.**' id(<audtaudt> authorized users) acc(r)  
pe 'CAI.TMS.**' id(VTAPE STCs)
```

```
ad 'CAI.TMS.**' uacc(none) owner(sys3) -  
    audit(success(update) failures(read)) -  
    data('CA CA-1 Install DS')  
pe 'CAI.TMS.**' id(<syspauDt> <tstcaudt>) acc(a)  
pe 'CAI.TMS.**' id(<audtaudt> authorized users) acc(r)  
pe 'CAI.TMS.**' id(CA-1 STCs)
```

setr generic(dataset) refresh

CCI: CCI-001499

Group ID (Vulid): V-17072

Group Title: ZB000003

Rule ID: SV-40071r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZCA1A003

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.

Responsibility: Information Assurance Officer

IACControls: DCSL-1, ECAR-1, ECAR-2, ECAR-3, ECCD-1, ECCD-2

Check Content:

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

- SENSITIVE.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 ACF2 data set access authorizations restricts READ access to application support personnel, production control and scheduling personnel, operations personnel, and auditors.

___ The ACF2 data set access authorizations restricts WRITE and/or greater

access to only systems programming personnel and tape management personnel.

____ The ACF2 data set access authorizations restricts UPDATE access is limited to CA 1 batch production jobs, and CA 1 started tasks.

____ The ACF2 data set access authorizations specify that all (i.e., failures and successes) ALTER access are 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. 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. ALTER 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 alter 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:

SET RULE

\$KEY(S3C)

\$PREFIX(SYS3)

CA1.AUDIT UID(<audtaudt>) R(A) E(A)

CA1.AUDIT UID(<operaudt>) R(A) E(A)

CA1.AUDIT UID(<pcspaudt>) R(A) E(A)

CA1.AUDIT UID(CA1 STCs) R(A) W(A) E(A)

CA1.AUDIT UID(<syspaudt>) R(A) W(A) A(L) E(A)

CA1.AUDIT UID(<tapeaudt>) R(A) W(A) A(L) E(A)

CA1.AUDIT UID(<tstcaudt>) R(A) W(A) A(L) E(A)

CA1.RDS UID(<syspaudt>) R(A) W(A) A(L) E(A)

CA1.RDS UID(<tapeaudt>) R(A) W(A) A(L) E(A)

CA1.RDS UID(<tstcaudt>) R(A) W(A) A(L) E(A)

CA1.TMC UID(<appspaudt>) R(A) E(A)

CA1.TMC UID(<audtaudt>) R(A) E(A)

CA1.TMC UID(<operaudt>) R(A) E(A)

CA1.TMC UID(<pcspaudt>) R(A) E(A)

CA1.TMC UID(CA1 STCs) R(A) W(A) E(A)

CA1.TMC UID(<syspaudt>) R(A) W(A) A(L) E(A)

CA1.TMC UID(<tapeaudt>) R(A) W(A) A(L) E(A)

CA1.TMC UID(<tstcaudt>) R(A) W(A) A(L) E(A)

CA1.VPD UID(<syspau<td>) R(A) W(A) A(L) E(A)

CA1.VPD UID(<tapeaudt>) R(A) W(A) A(L) E(A)

CA1.VPD UID(<tstcaudt>) R(A) W(A) A(L) E(A)

Review the authorizations to the CA1 TMC, AUDIT and optional RDS and VPD data sets. Ensure that the access granted to these data sets are in accordance with those outlined below.

Restrict users who need to access tape data set information (e.g., block size, counts) and information about creating jobs (e.g., jobname, stepname, or ddname) to the following:

READ access to the TMC, AUDIT and optional RDS and VPD data sets will be restricted to production support, operations, and auditing personnel. However, 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:

```
AD 'sys3.ca1.audit.**' UACC(NONE) OWNER(SYS3) AUDIT(SUCCESS(ALTER)
FAILURES(READ))
```

```
AD 'sys3.ca1.rds.**' UACC(NONE) OWNER(SYS3) AUDIT(SUCCESS(ALTER) FAILURES(READ))
```

AD 'sys3.ca1.tmc.**' UACC(NONE) OWNER(SYS2) AUDIT(SUCCESS(ALTER) FAILURES(READ))
AD 'sys3.ca1.vpd.**' UACC(NONE) OWNER(SYS3) AUDIT(SUCCESS(ALTER) FAILURES(READ))

PE 'sys3.ca1.audit.**' ID(audtaudt) ACC(R)
PE 'sys3.ca1.audit.**' ID(operaudt) ACC(R)
PE 'sys3.ca1.audit.**' ID(pcspaudt) ACC(R)
PE 'sys3.ca1.audit.**' ID(tmsinit) ACC(U)
PE 'sys3.ca1.audit.**' ID(syspaudt) ACC(A)
PE 'sys3.ca1.audit.**' ID(tapeaudt) ACC(A)
PE 'sys3.ca1.rds.**' ID(syspaudt) ACC(A)
PE 'sys3.ca1.rds.**' ID(tapeaudt) ACC(A)
PE 'sys3.ca1.tmc.**' ID(audtaudt) ACC(R)
PE 'sys3.ca1.tmc.**' ID(operaudt) ACC(R)
PE 'sys3.ca1.tmc.**' ID(pcspaudt) ACC(R)
PE 'sys3.ca1.tmc.**' ID(tmsinit) ACC(U)
PE 'sys3.ca1.tmc.**' ID(syspaudt) ACC(A)
PE 'sys3.ca1.tmc.**' ID(tapeaudt) ACC(A)
PE 'sys3.ca1.vpd.**' ID(syspaudt) ACC(A)
PE 'sys3.ca1.vpd.**' ID(tapeaudt) ACC(A)

CCI: CCI-000035

Group ID (Vulid): V-17947

Group Title: ZB000020

Rule ID: SV-40074r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZCA1A020

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.

Responsibility: Information Assurance Officer
IAControls: ECCD-1, ECCD-2

Check Content:

Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(CACMD)
- ACF2CMDS.RPT(RESOURCE) Alternate report

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 ACF2 resources and/or generic equivalent as designated in the

above table are defined with a default access of NONE.

___ The ACF2 resource access authorizations restrict access to the appropriate personnel as designated in the above table.

___ The ACF2 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 Resources for ACF2 tables in the zOS STIG Addendum. These tables list the resources, access requirements, and the resource type for CA 1 Command Resources; ensure the following guidelines are followed:

The ACF2 resources and/or generic equivalent as designated in the above table are defined with a default access of NONE.

The ACF2 resource access authorizations restrict access to the appropriate personnel as designated in the above table.

The ACF2 resource logging is specified as designated in the above table.

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

```
$KEY(LODELETE) TYPE(CAC)  
UID(tapeaudt) SERVICE(READ) ALLOW
```

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17982

Group Title: ZB000021

Rule ID: SV-40077r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZCA1A021

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.

Responsibility: Information Assurance Officer

IACControls: ECCD-1

Check Content:

Refer to the following report produced by the ACF2 Data Collection and Data Set

and Resource Data Collection:

- SENSITIVE.RPT(CATAPE)
- ACF2CMDS.RPT(RESOURCE) Alternate report

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 ACF2 resources and/or generic equivalent as designated in the above table are defined with a default access of NONE.

___ The ACF2 resource access authorizations restrict access to the appropriate personnel as designated in the above table.

___ The ACF2 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 ACF2 tables in the zOS STIG Addendum. These tables list the resources, access requirements, and the resource type for CA 1 Function and Password Resources; ensure the following guidelines are followed:

The ACF2 resources and/or generic equivalent as designated in the above table are defined with a default access of NONE.

The ACF2 resource access authorizations restrict access to the appropriate personnel as designated in the above table.

The ACF2 resource logging is specified as designated in the above table.

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

```
$KEY(BLPRES) TYPE(CAT)
UID(tapeaudt) SERVICE(READ,UPDATE) LOG
UID(syspautd) SERVICE(READ,UPDATE) LOG
```

CCI: CCI-000035

CCI: CCI-002234

Group ID (Vulid): V-17452

Group Title: ZB000030

Rule ID: SV-40080r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZCA1A030

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.

Responsibility: Information Assurance Officer

IAControls: ECCD-1, ECCD-2

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 SHUTDOWN 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 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):

```
au TMSINIT name('STC, CA 1 Tape Management') owner(stc) dfltgrp(stc) nopass
  data('Start CA1 TMS')
au CTS name('STC, CA 1 Common Tape System') owner(stc) dfltgrp(stc) nopass
  data(' CA Common Tape Service for CA1 - used to create tape labels')
```

CCI: CCI-000764

Group ID (Vulid): V-18014
Group Title: ZB000040
Rule ID: SV-40101r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCA1A040

Rule Title: CA 1 Tape Management external security options will 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.

Responsibility: Information Assurance Officer
IAControls: ECCD-1, ECCD-2

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 ACF2 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 - ACF2

Option Value

BATCH YES obsolete as of r12.0

CATSEC NO obsolete as of r12.0

CMD YES

CREATE see Note 1

DSNB YES

FUNC YES see Note 2

OCEOV NO see Note 3

PMASK Do not specify or change

PSWD YES

SCRATCH 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 ACF2 user LID record to allow access to BLP processing.

Note 3 The CA 1 security option, OCEOV, is set to NO because ACF2 obtains control of data set OPEN/CLOSE processing before the CA 1 intercept. The vendor recommends that the first security call be used and that this CA 1 control option be turned OFF. Therefore, TAPEDSN must be specified in the OPTS option in the ACF2 GSO 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.

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 - ACF2

Option	Value
BATCH	YES obsolete as of r12.0
CATSEC	NO obsolete as of r12.0
CMD	YES
CREATE	see note 1
DSNB	YES
FUNC	YES see note 2
OCEOV	NO see note 3
PMASK	Do not specify or change
PSWD	YES
SCRATCH	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 ACF2 user LID record

to allow access to BLP processing.

Note 3 The CA 1 security option, OCEOV, is set to NO because ACF2 obtains control of data set OPEN/CLOSE processing before the CA 1 intercept. The vendor recommends that the first security call be used and that this CA 1 control option be turned OFF. Therefore, TAPEDSN must be specified in the OPTS option in the ACF2 GSO 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

UNCLASSIFIED