

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

z/OS CA 1 Tape Management for RACF STIG

Version: 6

Release: 10

30 June 2023

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

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
IAControls: 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 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-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: ZB000000
 Rule ID: SV-40068r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCA1R000
 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
 IACControls: DCSL-1, ECAR-1, ECAR-2, ECCD-1, ECCD-2

Check Content:

a) Consult with your systems programmer to identify the names of the CA-1 product datasets. (They may begin with SYS2.CCS, SYS2A.CS., or SYS3.CCS).

b) Ensure the following data set controls are in effect for the CA-1 product data sets:

- UPDATE or higher access to the CA-1 product data sets is restricted to systems programming personnel.
- UACC (None) and NOWARNING are specified for the CA-1 product data sets..
- The RACF data set rules for the CA-1 data sets specify that all accesses of UPDATE or higher (i.e., failures and successes) will be logged.

c) Verify as follows:

1. From the Administrator main menu, select 3.3 (Dataset Profile Reports) and press ENTER
2. Tab down to Data Set row, type LV next to the dataset profile for the CA-1 data sets.
3. Check that UACC = None and Warning = No on the dataset profile General Information Screen.
4. Review the Universal Access and Access List on the dataset profile

General Information Screen..

5. Repeat steps 1-3 above for any other CA-1 dataset profiles.

d) If UPDATE and ALLOCATE (e.g. ALTER) access to the CA-1 product data sets are restricted to systems programming personnel, there is NO FINDING.

e) If UPDATE and ALLOCATE (ALTER) access to the CA -1 product data sets is not restricted to systems programming personnel, this is a FINDING.

f) If UACC = None and Warning = No there is NO FINDING

g) .IF UACC is not None or Warning is not No, this is a FINDING..

Fix Text: The IAO will 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.

Data sets to be protected will be:

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:

```
AD 'sys2.ca1.v**' UACC(NONE) OWNER(SYS2) AUDIT(SUCCESS(UPDATE)
FAILURES(READ))
```

```

AD 'sys2a.cal.v*.cailib.**' UACC(NONE) OWNER(SYS2A) AUDIT(SUCCESS(UPDATE)
FAILURES(READ))
AD 'sys2a.cal.v*.cailpa.**' UACC(NONE) OWNER(SYS2A) AUDIT(SUCCESS(UPDATE)
FAILURES(READ))
Or
AD 'sys2a.cal.v*.ctaplink.**' UACC(NONE) OWNER(SYS2A)
AUDIT(SUCCESS(UPDATE)
FAILURES(READ))
AD 'sys3.cal.**' UACC(NONE) OWNER(SYS3) AUDIT(SUCCESS(UPDATE)
FAILURES(READ))
AD 'sys3a.cal.v*.cailib.**' UACC(NONE) OWNER(SYS3A) AUDIT(SUCCESS(UPDATE)
FAILURES(READ))
Or
AD 'sys3a.cal.v*.ctaplink.**' UACC(NONE) OWNER(SYS3A)
AUDIT(SUCCESS(UPDATE)
FAILURES(READ))
AD 'sys3a.cal.v*.ctaplpa.**' UACC(NONE) OWNER(SYS3A)
AUDIT(SUCCESS(UPDATE)
FAILURES(READ))

PE 'sys2.cal.v**' ID(syspauDt) ACC(A)
PE 'sys2.cal.v**' ID(authorized users/*) ACC(R)
PE 'sys2a.cal.v*.cailib.**' ID(syspauDt) ACC(A)
PE 'sys2a.cal.v*.cailib.**' ID(authorized users/*) ACC(R)
PE 'sys2a.cal.v*.cailpa.**' ID(syspauDt) ACC(A)
PE 'sys2a.cal.v*.cailpa.**' ID(authorized users/*) ACC(R)
Or
PE 'sys2a.cal.v*.ctaplink.**' ID(syspauDt) ACC(A)
PE 'sys2a.cal.v*.ctaplink.**' ID(authorized users/*) ACC(R)
PE 'sys3.cal.v**' ID(syspauDt) ACC(A)
PE 'sys3.cal.v**' ID(authorized users/*) ACC(R)
PE 'sys3a.cal.v*.cailib.**' ID(syspauDt) ACC(A)
PE 'sys3a.cal.v*.cailib.**' ID(authorized users/*) ACC(R)
Or
PE 'sys3a.cal.v*.ctaplink.**' ID(syspauDt) ACC(A)
PE 'sys3a.cal.v*.ctaplink.**' ID(authorized users/*) ACC(R)
PE 'sys3a.cal.v*.ctaplpa.**' ID(syspauDt) ACC(A)
PE 'sys3a.cal.v*.ctaplpa.**' ID(authorized users/*) ACC(R)

```

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): ZCA1R001
 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
IAControls: 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:

- SENSITIVE.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(<syspau< <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(<syspau< <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): ZCA1R003
 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

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

Check Content:

a) Ensure that the CA-1 TMC and Audit data sets are properly protected and optional RDS and VPD data sets are properly protected. The RACF data set rule for the above data sets restrict READ access to The RACF data set rule for the above data sets restrict READ access to application support personnel, production control and scheduling personnel.

b) Based on Dataset Naming Conventions, identify effective masks to use to report on the TMC and Audit data sets. The low level qualifier of the data set names will probably be TMC and AUDIT respectively.

c) Once the masks are identified, from Administrator Main Menu, go to 3;3

Data Set Reports.

1. Select option 4 Access Lists, option B for Batch, and option Y for

Enhanced Masking, then ENTER

2. On the next panel enter the enhanced masking values separated by the

OR logic operand. E.g.

```
DATASET EQ SYS3.CA1.*TMC OR
```

```
DATASET EQ SYS3.CA1.*AUDIT
```

3. On the next panel enter a Y in the Explode RACF groups access list at

end of report field enter an N in all other fields, then ENTER .

4. Submit the Batch Job.

5. Review the output in the PRNT JES data set for the report.

d) The data set profiles listed above should restrict READ access to users with justification.

e) Only z/OS systems programmer and tape management personnel should have

UPDATE or higher access through these data set profiles.

f) In addition to z/OS systems programmers, Tape Librarians, CA 1 batch production batch jobs and CA 1 started tasks are allowed UPDATE access through these data set profiles.

g) From Administrator Main Menu, once again go to 3;3 Data Set Reports.

1. Select option 2 Audit Flags, option B for Batch, and option Y for Enhanced Masking, then ENTER .

2. On the next panel enter the enhanced masking values separated by the OR logic operand. E.g.

```
DATASET EQ SYS3.CA1.*TMC OR
D ATASET EQ SYS3.CA1.*AUDIT
```

3. Submit the Batch Job.

4. Review the output in the PRNT JES dataset for the report.

h) The data set profiles should specify successful ALTER access and all FAIL access attempts are logged.

i) If all of the items above are true, there are NO FINDINGS.

j) If any of the items above is untrue, there is one or more FINDINGS.

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. All alter access will be logged.

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): ZCA1R020
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:

- a) Ensure that all CA-1 command resources are properly protected.
- b) The CA-1 command resources RACF General Resource Class should be CA@MD. Once this has been verified, from Administrator Main Menu, go to 3;4 General Resource Reports.
 1. Select option 4 Access Lists, option B for Batch, and set the CLASS masking field to CA@MD, then ENTER .
 2. On the next panel enter a Y in the Explode RACF groups access list at end of report field, enter an N in all other fields, then ENTER .
 3. Submit the Batch Job.
 4. Review the output in the PRNT JES data set for the report.

c) Only the Tape Librarian should have READ access to the following profiles:

LOADD, LOCLEAN, LOCHECKI, LOCHECKO, LODELETE, LOERASE, LOEXPIRE, LORETAIN, LOSCRATC

d) Only the Tape Librarian and users requiring the functionality of extending retention dates for tape data sets should have READ access to the following profile:

LOEXTEND, LORETAIN

e) The Tape Librarian and Systems Programmers only have READ access to the following profile:

LOUPDTE

f) If all of the CA-1 command resources are protected at the appropriate levels, there is NO FINDING.

g) If any CA-1 command resource is not protected properly, there is a FINDING.

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

The RACF resource access authorizations restrict access to the appropriate

personnel as designated in the above table.

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

The RACF resource rules for the resources designated in the above table specify
UACC(NONE) and NOWARNING.

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

```
RDEFINE CA@MD L0DELETE UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
PERMIT L0DELETE CLASS(CA@MD) ACCESS(READ) ID(tapeaudt)
```

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): ZCA1R021
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
IAControls: ECCD-1

Check Content:

- a) Ensure that all CA-1 command resources are properly protected.
- b) The CA-1 command resources RACF General Resource Class should be

CA@MD. Once this has been verified, from Administrator Main Menu, go to 3;4

General Resource Reports.

- c). Select option 4 Access Lists, option B for Batch, and set the CLASS masking

field to CA@MD, then ENTER .

- d) On the next panel enter a Y in the Explode RACF groups access list at

end of report field, enter an N in all other fields, then ENTER .

- e) Submit the Batch Job.
- f) Review the output in the PRNT JES data set for the report.
- g) Only the Tape Librarian and Technical Support Personnel should have

READ and Update access to the following profiles:

NLRES, NLNORES, NSLRES

- h) Only the Tape Librarian and Systems Programmers should have READ and

UPDATE access to the following profiles:

NSLNORES, BLPRES, BLPNORES

- i) The Tape Librarian only should have READ and UPDATE access to the following profiles:

FORRES, YSVCUNCDC

- j) Systems Programmers should have READ access to the following profile:

YSVCUNCDC

- k) Systems Programmers and Operators would have access to the following profiles:

REINIT, BATCH, DEACT

- l) Users requiring access to CA-1 on-line applications for tape data set processing would have access through passwords. There are different passwords

for different levels of functionality from general user to tape librarian..

- m) If all of the CA-1 command resources are protected at the appropriate levels,

there is NO FINDING.

- n) If any CA-1 command resource is not protected properly, there is a FINDING.

****Note:** Tape librarian includes tape personnel, as well as STCs and Batch Users that perform CA 1 maintenance.

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

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

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

The RACF resource rules for the resources designated in the above table specify UACC(NONE) and NOWARNING.

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

```
RDEFINE CA@APE BLPRES UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
PERMIT BLPRES CLASS(CA@APE) ACCESS(UPDATE) ID(tapeaudt)
PERMIT BLPRES CLASS(CA@APE) ACCESS(UPDATE) ID(syspauadt)
```

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): ZCA1R030
 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
 IACControls: ECCD-1, ECCD-2

Check Content:

- a) From the Administrator main menu, select 3;4 (Security Server Reports - General Resource Reports) and press ENTER .
- b) Type 1 for General Resource Profile Summary and Tab down to CLASS: , type STARTED for class name.
- c).Find CA-1 started class General Resource profile usually named TMSINIT.
- d). Find the Userid associated with CA-1 started task under the STDATA segment information of the general resource profile.
- e). Go back to Administrator main menu, select 3;1 (Security Server Reports User Profile) and press ENTER .
- f) Tab down to User ID and enter the User ID found in Step d) above and hit enter.
- g). Page down till the Attributes section of the user profile.
- h) Verify that Protected = Yes.
- i) If Protected = Yes, there is no FINDING.
- j). If Protected = No, there is a FINDING.
- k) If TMSINIT is NOT found as a General Resource profile under the STARTED class in c. above, then check if is defined in the Started Procedures Table

(ICHRIN03) as follows:

- 1, From Analyzer main Menu, go to 3;4 (Online Displays Started Procedures Analysis) and Press ENTER
2. Look for STARTED in the Source column and TMSINIT in the Procname column..
3. If the TMSINIT started procedure does not have an R in the M column there is NO FINDING (an R in the M column indicates that either the STARTED TASK USER ID does not have the protected attribute or is not defined (these are both findings)
- 4..If there is an R in the M column, there is 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.

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-17454
 Group Title: ZB000032
 Rule ID: SV-40082r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCA1R032
 Rule Title: CA 1 Tape Management Started task will be 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) From the Administrator main menu, select 3;4 (Security Server Reports -

General

Resource Reports) and press ENTER .

b) Type 1 for General Resource Profile Summary and Tab down to CLASS: , type

STARTED for class name.

c). Find the general resources profile for the CA 1 started task, usually named TMSINIT.

d). If the General Resource profile for the CA 1 started task is found as a

General

under the STARTED class, there is no FINDING. .

e) If the General Resource profile for the CA 1 started task is not found in the

STARTED class, check if it is defined instead in the Started Procedures Table

(ICHRIN03) by running DSMON as a batch job or invoking it under TSO.

f). If the General Resource profile for the CA 1 started task IS found in the

Started Procedures Table (ICHRIN03) , there is NO FINDING.

g) If the General Resource profile for the CA 1 started task is NOT found in the

Started Procedures Table (ICHRIN03) either, this is a FINDING.

h) If TMSINIT is NOT found as a General Resource profile under the STARTED

class in d. above, then check if is defined in the Started Procedures Table

(ICHRIN03) as follows:

- 1, From Analyzer main Menu, go to 3;4 (Online Displays Started Procedures Analysis) and Press ENTER
2. Look for STARTED in the Source column and SDSF in the Procname column..
3. If SDSF is not found either as a General Resource Profile under STARTED class in e. above AND not found in the Started Procedures Table, this is 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 userid must be assigned for the CA 1 Tape Management started task(s) thru a corresponding STARTED class entry.

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

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

CCI: CCI-000764

Group ID (Vulid): V-18011
 Group Title: ZB000038
 Rule ID: SV-40668r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCA1R038
 Rule Title: CA 1 Tape Management Resource Class will be defined or active in the ACP.

Vulnerability Discussion: Failure to use a robust ACP to control a product could potentially compromise the integrity and availability of the MVS operating system and user data.

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

Check Content:

a) Find out from the users if they have defined their own RACF CLASSES for CA

1 resources.

b) Then verify if either the CA 1 RACF resource classes defined by the installation

or the default CA 1 resource classes are active as follows:

1) From the Administrator main menu, select 3;4 (Security Server Reports

- General Resource Reports) and press ENTER .

2) Type 1 for General Resource Profile Summary and Tab down to CLASS: , And enter either the installation-defined class names for CA 1 resources found

in step a. above or the default CA 1 resource class names (CA@CMD or CA@APE)

3). If the CLASS is found, there is no FINDING.

4). If the CLASS is not found, there is a FINDING. .

Fix Text: The IAO will ensure that the following CA 1 Tape Management Resource

Class(es) is (are) active.

CA@CMD

CA@APE

Use the following commands as an example:

SETROPTS CLASSACT(CA@MD,CA@APE)

CCI: CCI-000336

CCI: CCI-002358

Group ID (Vulid): V-18014

Group Title: ZB000040

Rule ID: SV-40101r1_rule

Severity: CAT II

Rule Version (STIG-ID): ZCA1R040

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:

a) Ensure that all CA 1 parameters meet the following requirements as specified in the U_zOS_STIG_Addendum. Note: You do not need to reassemble or execute the steps in these sections, just ensure that when CA-1 was installed the following conventions were observed.

b) Identify the CA-1 started procedure (STC) usually named TMSINIT.

c) Identify the two-character suffix for the TMOSYSxx member of the dataset referenced in the TMSPARM DD statement of the TMSINIT started procedure JCL (BY DEFAULT THE SUFFIX IS 00).

d) Identify the current TMSOPTxx member by browsing member TMOSYSxx of the dataset referenced in the TMSPARM DD statement of the TMSINIT started procedure JCL.

e) Identify the CA-1 PPOPTION dataset currently in use.

f) Browse member TMSOPTxx in the PPOPTION dataset currently in use.

Verify that the following parameters are set as follows:

BATCH	YES (applicable only to CA-1 Version 11.5 or below)
CATSEC	NO (applicable only to CA-1 Versions 5.3 to 11.5 (inclusive))
CMD	YES
CREATE	UPDATE
DSNB	YES
FUNC	YES

OCEOV NO

NOTE This requires the RACF System-wide TAPEDSN to be active.

PMASK	Do not specify or change
PSWD	YES
SCRATCH	NO
SECWTO	YES (applicable only to CA-1 Version 5.2

and
above)

UNDEF	FAIL
UX0AUPD	NO (applicable only to CA-1 Version 5.3 and

above)

YSVC	YES
------	-----

The systems programmer/IAO is responsible to ensure that the CA-1 external security options are specified in accordance with the above requirements.

g) If the settings are as specified above, there is NO FINDING.

h) If the settings are NOT specified as above, this is a FINDING

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 - RACF

OPTION	STANDARD VALUE
BATCH	YES obsolete as of r12.0
CATSEC	NO obsolete as of r12.0
CMD	YES
CREATE	UPDATE 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 vendor default setting for CREATE option is UPDATE to avoid volume serial number authorization verification. Otherwise, in an environment

where volume access rules are not utilized, user access will be denied when creating a tape data set.

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 vendor recommends that OCEOV be set to NO and the RACF SETROPTS option TAPEDSN be active. Be advised that if OCEOV is disabled and RACF TAPEDSN is not active, tape data set protection will not be in effect.

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