

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

z/OS TDMF for RACF STIG

Version: 6

Release: 4

20 Jan 2015

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

Group ID (Vulid): V-18014
Group Title: ZB000040
Rule ID: SV-24802r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZTDM0040
Rule Title: Transparent Data Migration Facility (TDMF)
configuration/parameter/option values are not specified properly.

Vulnerability Discussion: Transparent Data Migration Facility (TDMF) configuration/parameter/option settings control the security and operational characteristics of product. If these setting values are improperly specified, security and operational controls may be weakened. This exposure may threaten

the availability of the product applications, and compromise the confidentiality of system and customer data.

Responsibility: Systems Programmer

IACControls: ECCD-1, ECCD-2

Check Content:

a) Check with your IOA or Systems Programming personnel and compile the list of

Transparent Data Migration Facility (TDMF) Install data sets, Likely:

1. hlq.TDMF.**
2. From the Administrator Main Menu Choose Option 2;3 (Security Server Commands, Data Sets)
3. Type the resource names collected in option a.1 above at the prompt for Enter fully qualified (without quotes) data set or profile name:.
4. Hit enter.
5. Enter Y for Display covering profile? Y
6. Verify that the UACC is NONE
7. Verify that Audit Successes and Failures specifies UPDATE.
8. Tab down to Standard Access Permits and place an E next to the phrase and hit ENTER.

9. Verify that the data set rules for the product install data sets

- a. Permit READ access to all authorized users
- b. Restrict UPDATE or higher access to systems programming personnel.
10. Tab down to Conditional Access Permits line on the screen. If the phrase *data is present* is found, enter an E and hit ENTER.

11. Verify that any additional data set rules for the product install data sets

- a. Permit READ access only to authorized users
- b. Restrict UPDATE or higher access to systems programming personnel
12. Repeat steps 2 through 10 for all datasets in option a.1

b) If 10a, 10b, 12a, and 12b are all true, there is NO FINDING.

c) If 10a, 10b, 12a, and 12b are not true, this is a FINDING.

Fix Text: The product systems programmer will verify that any configuration / parameters that are required to control the security of the product are properly configured and syntactically correct.

See the required parameters below:

Parameter Options:
VOLUME SECURITY = YES
CHECK TARGET EMPTY = YES

Session Options:
Volume Security is not available.
CHECKTarget|CHKTarget

NOTE: The IAO will ensure that volume resource protection is define to the ACP and access to volumes be given to the appropiate personnel.

CCI: CCI-000035

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-24782r3_rule
Severity: CAT II
Rule Version (STIG-ID): ZTDMR000
Rule Title: Transparent Data Migration Facility (TDMF) installation data sets will be not properly protected.

Vulnerability Discussion: Transparent Data Migration Facility (TDMF) 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(TDMFRPT)

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

- PDI(ZTDM0000)

Verify that the accesses to the Transparent Data Migration Facility (TDMF) installation data sets are properly restricted. If the following guidance is true, this is not a finding.

____ 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 WRITE and/or greater access to systems programming personnel.

____ The RACF data set rules for the data sets specify that all (i.e., failures and successes) WRITE and/or greater access is logged.

____ The RACF data set rules for the data sets specify UACC(NONE) and NOWARNING.

Fix Text: The IAO will ensure that WRITE and/or greater access to Transparent Data Migration Facility (TDMF) installation data sets is limited to System Programmers only, and all WRITE and/or greater access is logged. READ access can be given to auditors.

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.TDMF.

SYS3.TDMF.

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

```
ad 'SYS2.TDMF.**' uacc(none) owner(sys2) -
    audit(success(update) failures(read)) -
    data('Transparent Data Migration Facility (TDMF) Install DS')
pe 'SYS2.TDMF.**' id(<syspautd> <tstcaudt>) acc(a)
pe 'SYS2.TDMF.**' id(<audtaudt>) acc(r)
```

```
ad 'SYS3.TDMF.**' uacc(none) owner(sys3) -
    audit(success(update) failures(read)) -
    data('Transparent Data Migration Facility (TDMF) Install DS')
pe 'SYS3.TDMF.**' id(<syspautd> <tstcaudt>) acc(a)
```

```
pe 'SYS3.TDMF.**' id(<audtaudt>) acc(r)
```

```
setr generic(dataset) refresh
```

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED