z/OS FDR for TSS STIG

Version: 6

Release: 2

20 Jan 2015

XSL Release 1/29/2015 Sort by: STIGID

Group ID (Vulid): V-18014
Group Title: ZB000040
Rule ID: SV-27074r1_rule
Severity: CAT I
Rule Version (STIG-ID): ZFDR0040
Rule Title: FDR (Fast Dump Restore) security options are improperly specified.

Vulnerability Discussion: Product configuration/parameters control the security and operational characteristics of products. If these parameter 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 customer data.

IAControls: ECCD-1, ECCD-2

Check Content:
a) The following steps are necessary for reviewing the FDR options:

1) Issue the following command on the command line at option 6 in TSO to bring up the FDR ISPF dialog:

EXEC 'SYS2.FDR.Vxxxx.CLIST(ABRALLOC)'

2) Select 'I' on the FDR primary panel for INSTALL.
3) Select '4' on the FDR installation options panel to select SETOPT.
4) Verify the FDR Program Library Data Set on this panel specifies the following:
Example: 'SYS2A.FDR.Vxxxx.LOADLIB'.
5) Select '1' for SECURITY OPTIONS.
6) Review the setting for ALLCALL

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

- PDI(ZFDR0040)

b) If ALLCALL is set to YES, there is NO FINDING.

c) If ALLCALL is set to NO, this is a FINDING.

Fix Text: The systems programmer will verify that the security option ALLCALL is set to Yes.

1) Execute the FDR ISPF dialog by entering the following on the command line:

EXEC 'SYS2.FDR.VXXXX.CLIST(ABRALLOC)'

2) Select 'I' on the FDR PRIMARY OPTIONS MENU for INSTALL.

3) Select '4' on the INSTALLATION OPTIONS MENU to select SETOPT - SET INSTALLATION OPTIONS IN THE FDR GLOBAL OPTIONS TABLE.

4) Verify the FDR program library data set on this panel is set to the current LOADLIB. Example: 'SYS2A.FDR.Vxxxx.LOADLIB'.

5) Select '1' to select SECURITY OPTIONS.

6) On the SET FDR GLOBAL SECURITY OPTIONS, review the ALLCALL setting, ensure it is set to YES.

CCI: CCI-000035

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-27205r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZFDRT000
Rule Title: Fast Dump Restore (FDR) install data sets are not properly protected.

Vulnerability Discussion: Fast Dump Restore (FDR) install have the ability to use privileged functions and/or have access to sensitive data. Failure to properly restrict access to their data sets could result in violating the integrity of the base product which could result in compromising the operating system or sensitive data.

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

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

- SENSITVE.RPT(FDRRPT)

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

- PDI(ZFDR0000)

b) Verify that access to the Fast Dump Restore (FDR) Install data sets are

properly restricted.

___ The TSS data set rules for the data sets does not restrict UPDATE and/or ALL access to systems programming personnel.

___ The TSS data set rules for the datasets does not specify that all (i.e., failures and successes) UPDATE and/or ALL access will be logged.

c) If all of the above are untrue, there is NO FINDING.

d) If any of the above is true, this is a FINDING.

Fix Text: The IAO will ensure that update and/or ALL access to Fast Dump Restore (FDR) install data sets is limited to System Programmers only, and all update and/or ALL access is logged. All other FDR users can have read access.

The installing Systems Programmer will identify and document the product data sets and categorize them according to who will have update and/or ALL access and if required that all update and/or ALL access is logged. He will identify if any additional groups have update and/or ALL 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.FDR
SYS2A.FDR

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

TSS PERMIT(syspaudt) DSN(SYS2.FDR.) ACCESS(R)
TSS PERMIT(syspaudt) DSN(SYS2.FDR.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<fdrusers>) DSN(SYS2.FDR.) ACCESS(R)

TSS PERMIT(syspaudt) DSN(SYS2A.FDR.) ACCESS(R)
TSS PERMIT(syspaudt) DSN(SYS2A.FDR.) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(<fdrusers>) DSN(SYS2A.FDR.) ACCESS(R)

CCI: CCI-000213

CCI: CCI-002234
