

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

z/OS FDR for RACF STIG

Version: 6

Release: 2

20 Jan 2015

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

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.

Responsibility: Systems Programmer

IACControls: 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

b) _If ALLCALL is set to YES, this is not a 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-27204r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZFDRR000
 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.

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

Check Content:

- a) Check with your IOA or Systems Programming personnel and compile the list of Fast Dump Restore installation datasets, Likely:
 1. hlq.FDR.**
 2. From the Administrator Main Menu choose Option 2 Security Server Commands
 3. then choose Option: 3 Data Set
 4. Type the resource names collected in option a.1 above into: Enter fully qualified (without quotes) data set or profile name:

5. Hit enter.
6. Enter Y for Display covering profile? Y
7. Verify that the UACC is NONE
8. Verify that Audit Successes and Failures specifies UPDATE or READ.

9. Tab down to Standard Access Permits and place an E next to it (hit enter)and
validate that UPDATE or higher access is limited to Systems Programming personnel
 10. if CONDITIONAL ACCESS PERMITS: _ (E to edit data) has *data is present* next to it, place an E next to it and validate that conditional access permits of Update or higher are limited to Systems Programming Personnel as well.
 11. Repeat steps 2 through 10 for all datasets in option a.1
- b) If a.7, a.8, a.9 and a.10 are all true, there is NO FINDING.
- c) If a.7, a.8, a.9 and a.10 are not true, this is a FINDING.

Fix Text: The IAO will ensure that update and allocate access to Fast Dump Restore (FDR) install data sets is limited to System Programmers only, and all update and allocate access is logged. Auditors should 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 alter access and if required that all update and allocate access is logged. He will identify if any additional groups have update 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:

```
ad 'sys2.fdr.**' uacc(none) owner(sys2) -
    audit(success(update) failures(read)) -
    data('Vendor DS Profile: fdr')
pe 'sys2.fdr.**' id(sypaudt) acc(a)
pe 'sys2.fdr.**' id(dasdaudt dasbaudt audtaudt) acc(r)
ad 'sys2a.fdr.**' uacc(none) owner(sys2a) -
    audit(success(update) failures(read)) -
    data('fdr Vendor Datasets')
pe 'sys2a.fdr.**' id(sypaudt) acc(a)
pe 'sys2a.fdr.**' id(dasdaudt dasbaudt audtaudt) acc(r)
ad 'sys3.fdr.**' uacc(none) owner(sys3) -
    audit(success(update) failures(read)) -
    data('Site Custom DS Profile: fdr')
```

```
pe 'sys3.fdr.**' id(syspautd) acc(a)  
pe 'sys3.fdr.**' id(dasdaudt dasbaudt audtaudt) acc(r)
```

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

CCI: CCI-000213

CCI: CCI002234

UNCLASSIFIED