z/OS Catalog Solutions for RACF STIG

Version: 6

Release: 5

30 June 2023

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

---

Group ID (Vulid):  V-16932
Group Title:  ZB000000
Rule ID:  SV-19581r2_rule
Severity: CAT II
Rule Version (STIG-ID):  ZCSLR000
Rule Title: Catalog Solutions Install data sets are not properly
protected.

Vulnerability Discussion:  Catalog Solutions is a very powerful tool that
can
pose risks if not properly controlled. If security is not properly
implemented,
the users of the product could present data integrity exposures, bypass
security
for catalog datasets, other VSAM files and alias s.

Catalog Solutions Install data sets provide the capability 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) Check with your IOA or Systems Programming personnel and compile the list of Fast Dump Restore installation datasets, Likely:
1. hlq.CSL.**
2. From the Administrator Main Menu Chose Option 2 Security Server Commands
3. then chose 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 lower (READ is acceptable)
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 program product data sets is limited to system programmers only, unless a letter justifying access is filed with the IAO, and all update and allocate access is 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 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.

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

```
ad 'sys2.csl.**' uacc(none) owner(sys2) -
 audit(success(update) failures(read)) -
 data('Catalog Solution Vendor Datasets: Ref SRR PDI ZCSLR000')
pe 'sys2.csl.**' id(<syspaudt>) acc(a)
ad 'sys3.csl.**' uacc(none) owner(sys3) -
 audit(success(update) failures(read)) -
 data('Catalog Solution Customized Datasets: Ref SRR PDI ZCSLR000')
pe 'sys3.csl.**' id(<syspaudt>) acc(a)
setr generic(dataset) refresh
```

Catalog Solution allows you to monitor your catalog environment to help identify and correct structural catalog problems before they create system outages. Catalog Solution is a valuable tool in planning for or implementing System Managed Storage, as well as ensuring daily system availability. Catalog Solution is a comprehensive facility for the management, maintenance, repair, and recovery of the MVS catalog environment that complements the IDC Access Method Services (IDCAMS) utility.

Catalog Solution helps you in the five key areas: Maintenance, Diagnostics, Reporting, Backup and Recovery, and SMF management.

Catalog Solution is a very powerful tool that can pose risks if not properly controlled. If security is not properly implemented, the users of the product could present data integrity exposures, bypass security for catalog datasets, other VSAM files and alias s. As an authorized program, Catalog Solution bypasses many of the normal system security facilities catalog and dataset passwords in particular. Improper use of Catalog Solution can result in non-synchronized catalog, dataset, or VVDS record groups. Therefore, certain commands should not be made available to the user community. As delivered, Catalog Solution bypasses dataset security checking for VSAM datasets and BCS processing. Clearly there are risks associated and valid requirements exist to ensure full external security controls are properly implemented for the Catalog Solution product.

Properly securing the use of various commands and features is crucial. All Catalog Solution functions should be reviewed for potential security exposures and to prevent unauthorized use. Some Catalog Solution functions allow for bypassing of security controls, and as such shall be restricted to system programmers who perform in the specific role of Storage management.

CCI: CCI-000213

CCI: CCI002234

Group ID (Vulid):  V-17947  
Group Title:  ZB000020  
Rule ID:  SV-19622r3_rule  
Severity: CAT II  
Rule Version (STIG-ID):  ZCSLR020  
Rule Title: Catalog Solutions resources are not properly defined and protected.

Vulnerability Discussion:  Catalog Solutions is a very powerful tool that can pose risks if not properly controlled. If security is not properly implemented, the users of the product could present data integrity exposures, bypass security for catalog datasets, other VSAM files and alias s. As an authorized program, Catalog Solution bypasses many of the normal system security facilities catalog and dataset passwords in particular. Improper use of Catalog Solution can result in non-synchronized catalog, dataset, or VVDS record groups. Therefore, certain commands should not be made available to the user community. As delivered, Catalog Solution bypasses dataset security checking for VSAM datasets and BCS processing. Clearly there are risks associated and valid requirements exist to ensure full external security controls are properly implemented for the Catalog Solutions product.

Properly securing the use of various commands and features is crucial to ensuring data integrity of the system.

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

Check Content:

Ensure the Catalogued Solutions Resources and / or generic equivalents are protected according to the requirements specified in the Catalog Solutions Resources table in the U_ZOS_STIG_Addendum.

a).        Do the following for all the PROFILES found in the Catalog Solutions Resources table in the U_ZOS_STIG_Addendum:

1.        From the Administrator Main Menu Choose Option 3 Security Server Reports

2.        Choose Option: 4 General Resource Profile

3.        On the command line choose option 4 and then enter hlq1* (see note below) of the Catalogued Solutions resources next to PROFILE and enter FACILITY next to CLASS.

4. Hit Enter.

5. Verify that the UACC for all profiles listed is NONE

6, Place an S next to the profile and validate that the access list is appropriate (as defined or more restrictive than the Catalog Solutions Resources table above). If TYPE is GROUP, place an S in the CMD line and hit enter to explode the GROUP.

7.        Repeat steps 6 and 7 for all PROFILES found in the Catalog Solutions Resources table in the U_ZOS_STIG_Addendum.

8 . For the hlq1.hlq2.GLOBAL.DATASET (see note below) profile, as it requires logging, also do the following - place an LR next to it, hit enter and review the output, and validate that it specifies ALL(READ).

9. For the hlq1.** (see note below) profile ensure that NO USERS have access other than NONE.

b). If all profiles, access lists, and logging are defined as or are more restrictive than what is defined in the Catalog Solutions Resources table in the U_ZOS_STIG_Addendum, then there is NO FINDING.

c). If any Profile, Access list or Logging specification is more permissive than what is permitted per the Catalog Solutions Resources table in the U_ZOS_STIG_Addendum, then there is a FINDING.

Note re hlq1: This is the high level qualifier for the resource. EMC is for software version 9.00 and below and ROCKET is for software version 9.10 and above.
Note re hlq2: This is the possible second high level qualifier for the resource. CSL is for software version 9.00 and below and RCS is for software version 9.10 and above.

Fix Text: Use the following recommendations when securing access to Catalog Solution Resources:

1) A RACF profile is defined for EMC.** with no users permitted access.

2) There is a RACF rule for EMC.CSL.GLOBAL.DATASET defined and only systems programming, DASD administration personnel, as well as any DASD batch users that need to bypass dataset security access checks may be permitted with READ access and access will be logged.

3) The RACF rules for each the following can be made available to all users at the IAOs discretion with the access of READ.

EMC.CSL.READ.CATLIST
EMC.CSL.READ.LIST

```
EMC.CSL.READ.SCAN
EMC.CSL.READ.PRINT
EMC.CSL.READ.ALIASCHK
EMC.CSL.READ.DIAGNOSE
```

4) The RACF rules for all profiles beginning with EMC.CSL.READ and EMC.CSL.UPDATE have restricted access to systems programming and DASD administration personnel as well as possibly any DASD batch users with access of READ.

5) All of the above RACF resources are defined with UACC(NONE).

A completed list of Catalog Solutions resources can be found in the z/OS STIG Addendum in the table titled "CATALOG SOLUTIONS Resource list"

Sample commands are provided here to implement the security requirements:

```
rdef facility emc.** uacc(none) owner(admin) audit(failure(read)) -
 data('added per PDI ZCSL0020')

rdef facility emc.csl.global.dataset uacc(none) owner(admin) -
 audit(all(read)) data('added per PDI ZCSL0020')
pe emc.csl.global.dataset cl(facility) id(<syspaudt>) acc(r)
pe emc.csl.global.dataset cl(facility) id(<dasdaudt>) acc(r)
pe emc.csl.global.dataset cl(facility) id(<dasbaudt>) acc(r)

/* At the IAOs discretion */
rdef facility emc.csl.read.catlist.** uacc(none) owner(admin) -
 audit(failure(read)) data('added per PDI ZCSL0020')
pe emc.csl.read.catlist.** cl(facility) id(*) acc(r)

/* At the IAOs discretion */
rdef facility emc.csl.read.list.** uacc(none) owner(admin) -
 audit(failure(read)) data('added per PDI ZCSL0020')
pe emc.csl.read.list.** cl(facility) id(*) acc(r)

/* At the IAOs discretion */
rdef facility emc.csl.read.scan.** uacc(none) owner(admin) -
 audit(failure(read)) data('added per PDI ZCSL0020')
pe emc.csl.read.scan.** cl(facility) id(*) acc(r)

/* At the IAOs discretion */
rdef facility emc.csl.read.print.** uacc(none) owner(admin) -
 audit(failure(read)) data('added per PDI ZCSL0020')
pe emc.csl.read.print.** cl(facility) id(*) acc(r)

/* At the IAOs discretion */
rdef facility emc.csl.read.aliaschk.** uacc(none) owner(admin) -
 audit(failure(read)) data('added per PDI ZCSL0020')
pe emc.csl.read.aliaschk.** cl(facility) id(*) acc(r)
```

```
/* At the IAOs discretion */
rdef facility emc.csl.read.diagnose.** uacc(none) owner(admin) -
 audit(failure(read)) data('added per PDI ZCSL0020')
pe emc.csl.read.diagnose.** cl(facility) id(*) acc(r)

/* NOTE THAT FURTHER GRANULARITY IS RECOMMENDED */
rdef facility emc.csl.read.** uacc(none) owner(admin) -
 audit(failure(read)) data('added per PDI ZCSL0020')
pe emc.csl.read.** cl(facility) id(<syspaudt>) acc(r)
pe emc.csl.read.** cl(facility) id(<dasdaudt>) acc(r)
pe emc.csl.read.** cl(facility) id(<dasbaudt>) acc(r)

/* NOTE THAT FURTHER GRANULARITY IS RECOMMENDED */
rdef facility emc.csl.update.** uacc(none) owner(admin) -
 audit(all(read)) data('added per PDI ZCSL0020')
pe emc.csl.update.** cl(facility) id(<syspaudt>) acc(r)
pe emc.csl.update.** cl(facility) id(<dasdaudt>) acc(r)
pe emc.csl.update.** cl(facility) id(<dasbaudt>) acc(r)

setr racl(facility) ref

.........................................
```

Product Information:

Catalog Solution allows you to monitor your catalog environment to help identify
and correct structural catalog problems before they create system outages.
Catalog Solution is a valuable tool in planning for or implementing System
Managed Storage, as well as ensuring daily system availability. Catalog Solution
is a comprehensive facility for the management, maintenance, repair, and
recovery of the MVS catalog environment that complements the IDC Access Method
Services (IDCAMS) utility.

Catalog Solution helps you in the five key areas: Maintenance, Diagnostics,
Reporting, Backup and Recovery, and SMF management.

Catalog Solution is a very powerful tool that can pose risks if not properly
controlled. If security is not properly implemented, the users of the product
could present data integrity exposures, bypass security for catalog datasets,
other VSAM files and alias s. As an authorized program, Catalog Solution
bypasses many of the normal system security facilities catalog and dataset
passwords in particular. Improper use of Catalog Solution can result in
non-synchronized catalog, dataset, or VVDS record groups. Therefore, certain

commands should not be made available to the user community. As delivered, Catalog Solution bypasses dataset security checking for VSAM datasets and BCS processing. Clearly there are risks associated and valid requirements exist to ensure full external security controls are properly implemented for the Catalog Solution product.

Properly securing the use of various commands and features is crucial. All Catalog Solutions functions should be reviewed for potential security exposures and to prevent unauthorized use. Some Catalog Solutions functions allow for bypassing of security controls, and as such shall be restricted to system programmers who perform in the specific role of Storage management.

CCI: CCI-000035

CCI: CCI-002234

UNCLASSIFIED