

# **VANGUARD**

**Integrity Professionals, Inc.**

---

**Enterprise Security Software**

z/OS Catalog Solutions for ACF2 STIG

Version: 6

Release: 4

20 Jan 2015

---

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

- SENSITIVE.RPT(CSLPROD)

Automated Analysis

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

- PDI(ZCSL0000)

b) Verify that access to the Catalog Solutions Install data sets are properly restricted.

\_\_\_ The ACF2 data set rules for the data sets does not restrict UPDATE and/or ALTER access to only systems programming personnel.

\_\_\_ The ACF2 data set rules for the data sets does not specify that all (i.e., failures and successes) UPDATE and/or ALTER 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 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 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.

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

SET RULE

\$KEY(S2C)

\$PREFIX(SYS2)

CSL.- UID(syspautd) R(A) W(L) A(L) E(A) DATA(DEFAULT SYSPROG)

\$KEY(S3C)

\$PREFIX(SYS3)

CSL.- UID(syspautd) R(A) W(L) A(L) E(A) DATA(DEFAULT SYSPROG)

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

IACControls: ECCD-1, ECCD-2

Check Content:

Refer to the following report produced by the ACF2 Data Collection and Data Set and Resource Data Collection:

- SENSITIVE.RPT(ZCSL0020)
- ACF2CMD5.RPT(RESOURCE) Alternate report

Automated Analysis

Refer to the following report produced by the Data Set and Resource Data

Collection:

- PDI(ZCSL0020)

Ensure that all Catalog Solutions resources and/or generic equivalents are properly protected according to the requirements specified in Catalog Solutions Resources table in the z/OS STIG Addendum. If the following guidance is true, this is not a finding.

\_\_\_ The ACF2 resources are defined with a default access of PREVENT.

\_\_\_ The ACF2 resource access authorizations restrict access to the appropriate personnel.

\_\_\_ The ACF2 resource logging is correctly specified.

Fix Text: The IAO will work with the systems programmer to verify that the following are properly specified in the ACP.

(Note: The resource type, resources, and/or resource prefixes identified below are examples of a possible installation. The actual resource type, resources, and/or resource prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.)

Ensure that all Catalog Solutions resources and/or generic equivalent are properly protected according to the requirements specified in Catalog Solutions Resources table in the z/OS STIG Addendum.

Use Catalog Solutions Resources table in the z/OS STIG Addendum. This table lists the resources, access requirements, and logging requirements for Catalogued Solutions. Ensure the following guidelines are followed:

The ACF2 resources are defined with a default access of PREVENT.

The ACF2 resource access authorizations restrict access to the appropriate personnel.

The ACF2 resource logging is correctly specified.

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

```
$KEY(hlq1) TYPE(FAC)
hlq2.GLOBAL.DATASET UID(dasdaudt) LOG
hlq2.GLOBAL.DATASET UID(dasbaudt) LOG
hlq2.GLOBAL.DATASET UID(syspauudt) LOG
hlq2.GLOBAL.DATASET UID(*) PREVENT
- UID(*) PREVENT
```

CCI: CCI-000035

CCI: CCI-002234

---

UNCLASSIFIED