VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

# z/OS Catalog Solutions for TSS STIG

Version: 6

Release: 4

20 Jan 2015

XSL Release 1/29/2015 Sort by: STIGID

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-19582r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCSLT000
Rule Title: Catalog Solution 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:

- SENSITVE.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 TSS data set rules for the data sets does not restrict UPDATE and/or ALTER access to systems programming personnel.

___ The TSS 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 ALL access to program product data

sets is limited to system programmers only, and all UPDATE and ALL 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 ALL access, and if required that all UPDATE and ALL 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:

TSS PERMIT(usracid) DSN(SYS2.CSL.) ACCESS(ALL) ACTION(AUDIT)

TSS PERMIT(usracid) DSN(SYS3.CSL.) ACCESS(ALL) ACTION(AUDIT)

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: CCI-002234

---

Group ID (Vulid): V-17947
Group Title: ZB000020
Rule ID: SV-19623r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZCSLT020
Rule Title: Catalog Solutions resources must be properly defined and protected.

Vulnerability Discussion: Catalog Solutions can run with sensitive system privileges, and potentially can circumvent system controls. Failure to properly control access to product resources could result in the compromise of the operating system environment, and compromise the confidentiality of customer data. Many utilities assign resource controls that can be granted to system programmers only in greater than read authority. Resources are also granted to certain non-systems personnel with read only authority.

IAControls: ECCD-1, ECCD-2

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

- SENSITVE.RPT(ZCSL0020)

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

- PDI(ZCSL0020)

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

___ The TSS resources and/or generic equivalent as designated in the above table are owned or DEFPROT is specified for the resource class.

___ The TSS resource access authorizations restrict access to the appropriate personnel as designated in the above table.

___ The TSS resource logging is specified as designated in the above

table.

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

(Note: The resource class, resources, and/or resource prefixes identified below are examples of a possible installation. The actual resource class, 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 Catalogued Solutions resources and/or generic equivalents are properly protected according to the requirements specified in Catalogued 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 TSS resources and/or generic equivalent as designated in the above table are owned or DEFPROT is specified for the resource class.

The TSS resource access authorizations restrict access to the appropriate personnel as designated in the above table.

The TSS resource logging is specified as designated in the above table.

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

TSS ADD(dept_acid) IBMFAC(hlq1)
TSS PERMIT(dasdaudt) IBMFAC(hlq1.hlq2.GLOBAL.DATASET) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(dasbaudt) IBMFAC(hlq1.hlq2.GLOBAL.DATASET) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(syspaudt) IBMFAC(hlq1.hlq2.GLOBAL.DATASET) ACCESS(ALL) ACTION(AUDIT)

CCI: CCI-000035

CCI: CCI-002234