VANGUARD
INTEGRITY PROFESSIONALS
INFORMATION SECURITY EXPERTS

z/OS VSS for RACF STIG

Version: 6

Release: 8

30 June 2023

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

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-24657r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZVSSR000
Rule Title: Vanguard Security Solutions (VSS) Install data sets are not properly protected.

Vulnerability Discussion: Vanguard Security Solutions (VSS) 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.

Responsibility: Information Assurance Officer
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 Vanguard Security Solutions (VSS) Install data sets, Likely:
1. hlq.VSS.
 hlq.VSS.VANOPTS
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. Verify that READ access is limited to Systems Programming Personnel, Security Personnel and Auditors.
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. Verify that READ access is limited to Systems Programming Personnel, Security Personnel and Auditors.
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 alter access to program product install data sets is limited to System Programmers, and read access is limited to Security personnel and Auditors, and all update and allocate access is logged.

The installing System 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 set prefix to be protected will be:

SYS2.VSS.
SYS2A.VSS.
SYS3.VSS.VANOPTS

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

```
ad 'sys2.vss.**' uacc(none) owner(sys2) -
 audit(success(update) failures(read)) -
 data('Vendor DS Profile: Vanguard Security Solutions')
pe 'sys2.vss.**' id(syspaudt) acc(a)
pe 'sys2.vss.**' id(secaaudt secdaudt audtaudt) acc(r)

ad 'sys2a.vss.**' uacc(none) owner(sys2a) -
 audit(success(update) failures(read)) -
 data('Vendor Loadlib: Vanguard Security Solutions')
pe 'sys2a.vss.**' id(syspaudt) acc(a)
pe 'sys2a.vss.**' id(secaaudt secdaudt audtaudt) acc(r)

ad 'sys3.vss.vanopts.**' uacc(none) owner(sys3) -
 audit(success(update) failures(read)) -
 data('Site Customized DS Profile: Vanguard Security Solutions')
pe 'sys3.vss.vanopts.**' id(syspaudt) acc(a)
pe 'sys3.vss.vanopts.**' id(secaaudt secdaudt audtaudt) acc(r)
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-21592
Group Title: ZB000002
Rule ID: SV-24915r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZVSSR002
Rule Title: Vanguard Security Solutions (VSS) User data sets are not properly

protected.

Vulnerability Discussion: Vanguard Security Solutions (VSS) User 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.

Responsibility: Information Assurance Officer
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 Vanguard Security Solutions (VSS) user data sets, Likely:
1. hlq.VSS.
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 READ, UPDATE, and/or ALTER access to systems programming personnel, security personnel, and auditors.
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 READ, UPDATE, and/or ALTER access to systems programming personnel, security personnel, and auditors.
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 read, update, and alter access to program product user data sets is limited to System Programmers, Security Personnel, and Auditors and all update and alter access is logged.

The installing System Programmer will identify and document the product user 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.

Data set prefix to be protected will be:

SYS3.VSS.

The above prefix can specify specific data sets, these would include the VSAM and JCL data sets. The following commands are provided as a sample for implementing dataset controls:

```
ad 'sys3.vss.**' uacc(none) owner(sys3) -
 audit(success(update) failures(read)) -
 data('Site Customized DS Profile: Vanguard Security Solutions')
pe 'sys3.vss.**' id(syspaudt secaaudt audtaudt) acc(a)
```

CCI: CCI-001499

Group ID (Vulid): V-17947
Group Title: ZB000020
Rule ID: SV-24912r2_rule
Severity: CAT II
Rule Version (STIG-ID): ZVSSR020
Rule Title: Vanguard Security Solutions' resources for the FACILITY resource class are not properly defined and protected.

Vulnerability Discussion: Program products can run with sensitive system privileges, and potentially can circumvent system controls. Failure to properly control access to program 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 sytems personnel with read only authority.

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

Check Content:

a) Verify the resources identified in the Vanguard Security Solutions Resources table in the zOS STIG Addendum are properly defined and access is restricted to the appropriate personnel.
For all the PROFILES found in VANGUARD SECURITY SOLUTIONSvRESOURCE TABLE in the zOS STIG Addendum:

1. From the Administrator Main Menu choose Option 3 Security Server Reports
2. then choose Option: 4 General Resource Profile
3. On the command line choose option 4 AND then Put (VRA*, VSA* or VSR*) next to PROFILE: and FACILITY next to CLASS depending on which resources you are checking from the VANGUARD SECURITY SOLUTIONS RESOURCE TABLE above. Also check IRR.PASSWORD.RESET and VIP$.NOEDIT.COMMANDS profiles.

Profile: VRA*
Class: FACILITY
 Or
Profile: VSA*
Class: FACILITY
 Or
Profile: VSR*
Class: FACILITY

4. Hit enter.
5. Verify that the UACC for all profiles listed is NONE and NOWARNING
6. Place an S next to the profile and validate that the access list is appropriate (as defined or more restrictive than the VANGUARD SECURITY SOLUTIONS RESOURCE TABLE above). If TYPE is GROUP, place an S in the CMD line and hit enter to explode the GROUP.
 NOTE: The RACF resource VSR$.SCOPE is allowed READ access when approved and documented by ISSM or equivalent Security Authority.
7. For all resources with logging requirements place an LR next to the profile (hit enter and review the output) and validate that it matches the logging requirement in the table.

b) If all profiles, access lists, and Auditing are defined like or more restrictively than in the

VANGUARD SECURITY SOLUTIONS RESOURCE TABLE above, then there is NO FINDING.

c) If any Profile, Access list or Auditing is more permissive than VANGUARD SECURITY SOLUTIONS RESOURCE TABLE above, then there is a FINDING.

Fix Text: Configure ACP resource definitions in accordance with Vanguard Security Solutions Resources and Vanguard Security Solutions Resources Descriptions tables in the zOS STIG Addendum. These tables list the resources, descriptions, and access and logging requirements. Ensure the guidelines for the resources and/or generic equivalent specified in the z/OS STIG Addendum are followed.

(Note: The resources, and/or resource prefixes identified below are examples of a possible installation. The actual 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.)

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

```
rdef facility vra$.acstask.** uacc(none) owner(admin)
audit(all(read)) -
data('protected per zvssr020')

pe vra$.acstask.** cl(facility) id(<audtaudt>) acc(read)
pe vra$.acstask.** cl(facility) id(<secaaudt>) acc(read)
Sample scope definition:
rdef facility vsr$.** uacc(none) owner(admin) audi(a(r)) -
 data('deny-by-default for Vanguard Advisor Reporter')
rdef facility vsr$.scope uacc(none) owner(admin) -
 audit(a(u)) data('Vanguard Advisor Reporter Auth Scope')
```

CCI: CCI-000035

CCI: CCI-002234

UNCLASSIFIED