

**UNCLASSIFIED**

**VANGUARD**  
**INTEGRITY PROFESSIONALS**  

---

**INFORMATION SECURITY EXPERTS**

**z/OS SRRAUDIT for RACF  
STIG**

**Version: 7**

**Release: 2**

**03 Mar 2026**

**Description:**

---

**Group ID (Vulid):** V-16932**Group Title:** ZB000000**Rule ID:** SV-21732r2\_rule**Severity:** CAT II**Rule Version (STIG-ID):** [ZSRRR000](#)**Rule Title:** SRRAUDIT Install data sets are not properly protected.

**Vulnerability Discussion:** SRRAUDIT 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 SRRAUDIT installation datasets, Likely:

1. hlq.SRRAUDIT.\*\*
  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. READ access is allowed for Systems Programming  
personnel,  
domain level production control and scheduling personnel, and  
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. READ access is allowed for 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 alter 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 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:

SYS2.SRRAUDIT.

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

```
ad 'sys2.srraudit.**' uacc(none) owner(sys2) -  
audit(success(update) failures(read)) -  
data('Vendor DS Profile: SRRAUDIT -  
security automation project, sso-developed self-audit toolkit')  
pe 'sys2.srraudit.**' id(syspauDt) acc(a)  
pe 'sys2.srraudit.**' id(secaudt audtaudt) acc(r)
```

**CCI:** CCI-000213

**CCI:** CCI-002234

---

**Group ID (Vulid):** V-21592

**Group Title:** ZB000002

**Rule ID:** SV-23903r2\_rule

**Severity:** CAT II

**Rule Version (STIG-ID):** [ZSRRR002](#)

**Rule Title:** SRRAUDIT User data sets are not properly protected.

**Vulnerability Discussion:** SRRAUDIT 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.

**IAControls:** DCSL-1, ECAR-1, ECAR-2, ECCD-1, ECCD-2

## Check Content:

b) Check with your IOA or Systems Programming personnel and compile the list of SRRAUDIT USER datasets, Likely:

1. hlq.SRRAUDIT.\*\*
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 the RACF data set rules for the data sets restricts  
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 for the data sets restricts 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.SRRAUDIT.

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

```
ad 'sys3.srraudit.**' uacc(none) owner(sys3) -  
audit(success(update) failures(read)) -  
data('Vendor DS Profile: SRRAUDIT -  
security automation project, sso-developed self-audit toolkit')  
pe 'sys3.srraudit.**' id(syspau dt secaa udt audta udt) acc(a)
```

If doing a full SRR review using the z/OS STIG Instruction, the following data set prefix to be protected will be:

SYS3.FSO.

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

```
ad 'sys3.fso.**' uacc(none) owner(sys3) -  
audit(success(update) failures(read)) -  
data('Used for full SRR Review')  
pe 'sys3.fso.**' id(syspau dt secaa udt audta udt) acc(a)
```

**CCI:** CCI-001499

---

**UNCLASSIFIED**