



CVE-2023-31150

Published on: Not Yet Published

Last Modified on: 05/17/2023 07:36:00 PM UTC

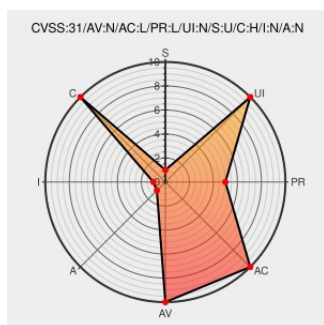
CVE-2023-31150

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Sel-2241 Rtac Module](#) from [Selinc](#) contain the following vulnerability:

A Storing Passwords in a Recoverable Format vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) database system could allow an authenticated attacker to retrieve passwords. See SEL Service Bulletin dated 2022-11-15 for more details.

CVE-2023-31150 has been assigned by security@selinc.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVE References

Description	Tags	Link
Security Notifications - Issues Reported by External Organization or Individuals	selinc.com text/html	MISC selinc.com/support/security-notifications/external-reports/
OT & IoT Security Blog – Nozomi Networks	www.nozominetworks.com text/html	MISC www.nozominetworks.com/blog/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Selinc	Sel-2241 Rtac Module	-	All	All	All
Operating System	Selinc	Sel-2241 Rtac Module Firmware	All	All	All	All
Hardware 	Selinc	Sel-3350	-	All	All	All
Operating System	Selinc	Sel-3350 Firmware	All	All	All	All
Hardware 	Selinc	Sel-3505	-	All	All	All
Hardware 	Selinc	Sel-3505-3	-	All	All	All
Operating System	Selinc	Sel-3505-3 Firmware	All	All	All	All
Operating System	Selinc	Sel-3505 Firmware	All	All	All	All
Hardware 	Selinc	Sel-3530	-	All	All	All
Hardware 	Selinc	Sel-3530-4	-	All	All	All
Operating System	Selinc	Sel-3530-4 Firmware	All	All	All	All
Operating System	Selinc	Sel-3530 Firmware	All	All	All	All
Hardware 	Selinc	Sel-3532	-	All	All	All
Operating System	Selinc	Sel-3532 Firmware	All	All	All	All
Hardware 	Selinc	Sel-3555	-	All	All	All
Operating System	Selinc	Sel-3555 Firmware	All	All	All	All
Hardware 	Selinc	Sel-3560e	-	All	All	All
Operating System	Selinc	Sel-3560e Firmware	All	All	All	All
Hardware 	Selinc	Sel-3560s	-	All	All	All
Operating System	Selinc	Sel-3560s Firmware	All	All	All	All
cpe:2.3:h:selinc:sel-2241_rtac_module:-:*~::~~::~:						
cpe:2.3:o:selinc:sel-2241_rtac_module_firmware:*~::~~::~:						
cpe:2.3:h:selinc:sel-3350:-:*~::~~::~:						
cpe:2.3:o:selinc:sel-3350_firmware:*~::~~::~:						
cpe:2.3:h:selinc:sel-3505:-:*~::~~::~:						

cpe:2.3:h:selinc:scl-3505-3:-:*:*:*:*:*:
cpe:2.3:o:selinc:scl-3505-3_firmware:*:*:*:*:*:
cpe:2.3:o:selinc:scl-3505_firmware:*:*:*:*:*:
cpe:2.3:h:selinc:scl-3530:-:*:*:*:*:*:
cpe:2.3:h:selinc:scl-3530-4:-:*:*:*:*:*:
cpe:2.3:o:selinc:scl-3530-4_firmware:*:*:*:*:*:
cpe:2.3:o:selinc:scl-3530_firmware:*:*:*:*:*:
cpe:2.3:h:selinc:scl-3532:-:*:*:*:*:*:
cpe:2.3:o:selinc:scl-3532_firmware:*:*:*:*:*:
cpe:2.3:h:selinc:scl-3555:-:*:*:*:*:*:
cpe:2.3:o:selinc:scl-3555_firmware:*:*:*:*:*:
cpe:2.3:h:selinc:scl-3560e:-:*:*:*:*:*:
cpe:2.3:o:selinc:scl-3560e_firmware:*:*:*:*:*:
cpe:2.3:h:selinc:scl-3560s:-:*:*:*:*:*:
cpe:2.3:o:selinc:scl-3560s_firmware:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
🔒 @CVEreport	CVE-2023-31150 : A Storing Passwords in a Recoverable Format vulnerability in the Schweitzer Engineering Laborator... twitter.com/i/web/status/1...	2023-05-10 20:05:53

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report