



Semtech LR11xx Memory Write Access Control Bypass

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2025-14857
State	PUBLISHED
Assigner	SWI
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 20:16:21 UTC
Updated	2026-04-08 21:27:00 UTC
Description	An improper access control vulnerability exists in Semtech LoRa LR11xxx transceivers running early versions of firmware w

Risk And Classification

Primary CVSS: v4.0 5.4 MEDIUM from security@sierrawireless.com

CVSS:4.0/AV:P/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:N/R:A/V:D/RE:M/U:X

EPSS: 0.000250000 probability, percentile 0.070560000 (date 2026-04-13)

Problem Types: CWE-123 | CWE-123 CWE-123 Write-what-where Condition

Version	Source	Type	Score	Severity	Vector
4.0	security@sierrawireless.com	Secondary	5.4	MEDIUM	CVSS:4.0/AV:P/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:N/R:A/V:D/RE:M/U:X
4.0	CNA	CVSS	5.4	MEDIUM	CVSS:4.0/AV:P/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:N/R:A/V:D/RE:M/U:X

CVSS v4.0 Breakdown

Attack Vector

Physical

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:P/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:N/R:A/V:D/RE:M/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Semtech	LR1110	affected TRX FW 0x0402 custom	Not specified
CNA	Semtech	LR1120	affected TRX FW 0x0202 custom	Not specified
CNA	Semtech	LR1121	affected TRX FW 0x0104 custom	Not specified

References

Reference	Source	Link	Tags
www.semtech.com/company/security/security-bulletins/sem-psa-2026-001	security@sierrawireless.com	www.semtech.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

Vendor Comments And Credit

Discovery Credit

CNA: Egor (radioegor146) Koleda, <https://github.com/radioegor146> (en)

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

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](#).

Free CVE JSON API cve.report/api

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