Semtech LR11xx Secure Boot Bypass

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-14859
State	PUBLISHED
Assigner	SWI
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 20:16:22 UTC
Updated	2026-04-08 21:27:00 UTC
Description	The Semtech LR11xx LoRa transceivers implement secure boot functionality using digital signatures to authenticate firmwa

Risk And Classification

Primary CVSS: v4.0 7 HIGH from security@sierrawireless.com

CVSS:4.0/AV:P/AC:L/AT:N/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/MSC:X/MSI:X/MSA:X/S:X/AU:N/R:I/V:C/RE:M/U:X

EPSS: 0.000100000 probability, percentile 0.011450000 (date 2026-04-13)

Problem Types: CWE-327 | CWE-327 CWE-327 Use of a Broken or Risky Cryptographic Algorithm

Version	Source	Type	Score	Severity	Vector
4.0	security@sierrawireless.com	Secondary	7	HIGH	CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/S/
4.0	CNA	CVSS	7	HIGH	CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/S/

CVSS v4.0 Breakdown

Attack Vector

Physical

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

ntegrity

High

vailability

High

ub Conf.

Low

ub Integrity

Low

ub Availability

None

CVSS:4.0/AV:P/AC:L/AT:N/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/MSC:X/MSI:X/MSA:X/S:X/AU:N/R:I/V:C/RE:M/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Semtech	LR1110	affected BL2 FW 0x1001 custom	Not specified
CNA	Semtech	LR1120	affected BL2 FW 0x2001 custom	Not specified
CNA	Semtech	LR1121	affected BL2 FW 0x2101 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

No vendor comments have been submitted for this CVE.

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