Product Security Advisory: LR11xx

Semtech Advisory: SEM-PSA-2026-001

Revision	Date	Notes
R1	7 April 2026	Initial Release

Summary

Semtech was made aware of two security vulnerabilities (CVE-2025-14857 and CVE-2025-14858) and internally discovered a third vulnerability (CVE-2025-14859) that affects certain Semtech LoRa transceivers and modems. These vulnerabilities could allow unauthenticated firmware to be loaded and executed on affected devices. These vulnerabilities require physical access to exploit and cannot be leveraged remotely.

Affected Products

- LR1110 running TRX FW versions earlier than 0x0402 and BL2 FW versions earlier than 0x1001
- LR1120 running TRX FW versions earlier than 0x0202 and BL2 FW versions earlier than 0x2001
- LR1121 running TRX FW versions earlier than 0x0104 and BL2 FW versions earlier than 0x2101

Risk Assessment

These vulnerabilities could be used together or separately to allow unauthenticated firmware to be loaded and executed on affected devices.
However, the vulnerabilities require physical access and are not remotely exploitable. Devices that are physically secured and connected to non-compromised host systems are protected from exploitation. Furthermore, the vulnerabilities do not disclose cryptographic keys as these are isolated by the onboard crypto engine.

Recommendations

Customers are advised to:

- Apply firmware updates promptly. https://github.com/Lora-net/SWTL001
- Ensure physical security measures are in place for deployed devices.
- Monitor host systems for signs of compromise.

Additional Resources

https://github.com/Lora-net/radio_firmware_images/tree/master/lr1110/transceiver
https://github.com/Lora-net/radio_firmware_images/tree/master/lr1120/transceiver
https://github.com/Lora-net/radio_firmware_images/tree/master/lr1121/transceiver
https://github.com/Lora-net/radio_firmware_images/tree/master/lr1121/modem
https://github.com/Lora-net/radio_firmware_images/tree/master/lr1110/modem
https://github.com/Lora-net/SWDR001
https://github.com/Lora-net/lr1121_modemE_driver
https://github.com/Lora-net/SWTL001

Details

CVE ID	Description	CVSSv4.0	Severity
CVE-2025-14857	An improper access control vulnerability exists in Semtech LoRa LR11xxx transceivers running early versions of firmware where the memory write command accessible via the physical SPI interface fails to enforce write protection on the program call stack. An attacker with physical access to the SPI interface can overwrite stack memory to hijack program control flow and achieve limited arbitrary code execution.	5.4	Medium
CVE-2025-14858	The Semtech LR11xx LoRa transceivers running early versions of firmware contains an information disclosure vulnerability in its firmware validation functionality. When a host issues a firmware validity check command via the SPI interface, the device decrypts the provided encrypted firmware package block-by-block to validate its integrity. However, the last decrypted firmware block remains uncleared in memory after the validation process completes. An attacker with access to the SPI interface can subsequently issue memory read commands to retrieve the decrypted firmware contents from this residual memory, effectively bypassing the firmware encryption protection mechanism. The attack requires physical access to the device's SPI interface.	5.1	Medium
CVE-2025-14859	The Semtech LR11xx LoRa transceivers implement secure boot functionality using digital signatures to authenticate firmware. However, the implementation uses a non-standard cryptographic hashing algorithm that is vulnerable to second preimage attacks. An attacker with physical access to the device can exploit this weakness to generate a malicious firmware image with a hash collision, bypassing the secure boot verification mechanism and installing arbitrary unauthorized firmware on the device.	7.0	High