



Product Security Advisory: LR11xx

Semtech Advisory: SEM-PSA-2026-002

Revision	Date	Notes
R1	12 October 2026	Initial Release

Summary

Semtech was made aware of a security vulnerability (CVE-2026-6232) that affects certain Semtech LoRa transceivers and modems. This vulnerability could allow arbitrary writes of up to 254 arbitrary bytes past the bounds of an internal, non-persistent memory buffer. These vulnerabilities require physical access to exploit and cannot be leveraged remotely.

The issue is fixed in the latest LR11xx transceiver firmware releases:

- LR1110 0x0403
- LR1120 0x0203
- LR1121 0x0105

The issue is also fixed in the latest LR1110 and LR1121 modem-e firmware releases (LR1120 does not support modem-e):

- LR1110 v2.1.1
- LR1121 v2.1.1

The fix is also incorporated into the LR11xx transceiver production firmware lines (these do not have earlier versions):

- LR1110 A1_0303
- LR1120 A2_0101
- LR1121 A3_0101

Affected Products

- LR1110 Transceiver running firmware versions earlier than 0x0403
- LR1110 Modem-e running firmware versions earlier than v2.1.1
- LR1120 Transceiver running firmware versions earlier than 0x0203
- LR1121 Transceiver running firmware versions earlier than 0x0105
- LR1121 Modem-e running firmware versions earlier than v2.1.1

Risk Assessment

This vulnerability could be used to influence the behaviour of the firmware including creating a crash.



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 arbitrary bytes are non-persistent and the firmware will recover after a reboot.

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-2026-6232	An out-of-bounds write vulnerability in the SPI host command interface of Semtech's LR11xx transceiver firmware where a crafted SPI host command with an oversized length field can cause the firmware to write up to 254 arbitrary bytes past the bounds of an internal, non-persistent memory buffer. Exploitation requires physical access to the device and logical access to the SPI bus.	5.2	Medium