Product Security Advisory: ALEOS Buffer Overflow and Filesystem Disclosure

Sierra Wireless Advisory SWI-PSA-2021-001 (link to latest version)

Date of issue: January 18, 2021

Summary

Sierra Wireless has confirmed two security issues in ALEOS.

Affected Products

CVE-2019-11851 applies to the following AirLink products:

- MP70, MP70E, RV50, RV50X, LX40 and LX60 running ALEOS 4.13.0 and earlier
- GX450 and ES450 running ALEOS 4.9.4 and earlier
- LS300, GX400, GX440 and ES440 running ALEOS 4.4.8 and earlier

This vulnerability is fixed in ALEOS 4.14.0, ALEOS 4.9.5, and ALEOS 4.4.9.

CVE-2019-11857 applies to the following AirLink products:

- MP70, MP70E, RV50, RV50X, LX40 and LX60 running ALEOS 4.11.2 and earlier
- GX450 and ES450 running ALEOS 4.9.4 and earlier
- LS300, GX400, GX440 and ES440 running ALEOS 4.4.8 and earlier

This vulnerability is fixed in ALEOS 4.12.0, ALEOS 4.9.5, and ALEOS 4.4.9.

Scope of Impact

ALEOS ACENet Buffer Overflow

A buffer overflow exists in the ACENet service, and this buffer overflow may allow remote code execution on some devices. The ACENet service is enabled by default on the WAN interface in ALEOS versions prior to 4.9.0, and is enabled by default only on the LAN interfaces in ALEOS 4.9.0 and later.

CVE-2019-11851 has been assigned to this issue, with the title “ALEOS ACENet Buffer Overflow.” Sierra Wireless has assigned a CVSSv3.0 score of 5.3 (Medium) based on the vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L.

ALEOS Filesystem Disclosure

An authenticated user can use a crafted input to read sensitive files from the ALEOS filesystem.

CVE-2019-11857 has been assigned to this issue, with the title "ALEOS Filesystem Disclosure." Sierra Wireless has assigned a CVSSv3.0 score of 4.4 (Medium) based on the vector CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N.

Recommended Actions

Sierra Wireless recommends upgrading to the latest ALEOS version for your gateway.

For devices that cannot be upgraded that are running ALEOS 4.9.0 and later, Sierra Wireless recommends setting "Services: ALMS: HTTP Server And ACEview Services" to "Disable."

Credits

CVE-2019-11857 "ALEOS Filesystem Disclosure" was reported by New York City Cyber Command.

Support Contact Information

Sierra Wireless Technical Support is available by phone or web portal from 6:00 to 17:00 PST, Monday to Friday.

Phone (Toll Free): 1-877-687-7795

Web: https://www.sierrawireless.com/support/community-portal/

Security Bulletins

To see the latest security updates from Sierra Wireless, please visit:

https://www.sierrawireless.com/company/security/