Technical Bulletin: ALEOS Security Update

Sierra Wireless Advisory SWI-PSA-2020-004 (link to latest version)

Date of issue: August 7, 2020

Summary

This technical bulletin covers fixes for multiple ALEOS security issues found through internal testing and customer audits.

Affected Products

This bulletin applies to the following AirLink products:

- MP70, MP70E, RV50, RV50X, LX40 and LX60 running ALEOS 4.12 and earlier
- GX450 and ES450 running ALEOS 4.9.4 and earlier
- LS300, GX400, GX440 and ES440 running ALEOS 4.4.8 and earlier

Scope of Impact

The following table summarizes the vulnerabilities found, their assigned CVSSv3 severity scores and the version(s) in which each vulnerability has been fixed.

CVE	CVSSv3.0 Score	Summary	ALEOS Fix Version(s)
CVE-2019-11857	9.1	ALEOS AceManager Information Disclosure: Lack of input sanitization in AceManager allows disclosure of sensitive system information.	4.12.0 4.9.5 4.4.9
CVE-2019-11855	8.1	ALEOS LAN-Side RPC Server: An RPC server is enabled by default on the gateway LAN.	4.12.0 4.9.5 4.4.9
CVE-2019-11847	7.3	ALEOS User Root Shell Escalation: An authenticated user can escalate to root via the command shell.	4.11.0 4.9.4 4.4.9
CVE-2019-11849	6.3	ALEOS AT API Stack Overflow: A stack overflow in the AT command APIs may allow code execution.	4.11.0
CVE-2019-11850	6.3	ALEOS AT Command Stack Overflow: A stack overflow in the AT command interface may allow code execution.	4.11.0

CVE-2019-11859	6.0	ALEOS SMS Handler Buffer Overflow: A buffer overflow exists in the SMS handler API that may allow code execution as root.	4.13.0 4.9.5 4.4.9
CVE-2019-11858	5.7	ALEOS Multiple Web UI vulnerabilities: The AceManager Web API has multiple buffer overflow vulnerabilities.	4.13.0 4.9.5 4.4.9
CVE-2019-11848	4.1	ALEOS AT Command API Abuse: An overflow is possible due to lack of length checking when handling certain user-provided values.	4.13.0 4.9.5 4.4.9
CVE-2019-11853	3.9	ALEOS AT Command Injections: Several potential command injections exist in the AT command interface.	4.11.0 4.9.4
CVE-2019-11852	3.7	ALEOS ACEView Service Out-Of-Bounds Read: Sensitive information may be disclosed via the ACEview service, accessible by default on the LAN.	4.13.0 4.9.5 4.4.9
CVE-2019-11856	3.3	ALEOS ACEView Message Replay: Captured traffic to the ACEView service can be replayed to other gateways sharing the same credentials.	4.13.0 4.9.5 4.4.9

Recommended Actions

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

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/