Product Security Advisory: AirLink ALEOS Security Update

Sierra Wireless Advisory SWI-PSA-2021-006 (link to latest version)

Date of issue: November 18, 2021

Summary

This technical bulletin covers fixes for multiple ALEOS security issues. These issues were found through internal testing by Sierra Wireless.

Affected Products

This bulletin applies to the following AirLink products:

- MP70, MP70E, RV50, RV50X, LX40 and LX60 running ALEOS 4.14.0 and earlier (see list for some issues fixed in 4.14.0)
- GX450 and ES450 running ALEOS 4.9.5 and earlier
- LS300, GX400, GX440 and ES440 running ALEOS 4.4.9 and earlier

One issue, CVE-2021-36733, only affects GX450 running ALEOS 4.9.5 and earlier.

Scope of Impact

The following table summarizes the vulnerabilities found, their assigned CVSSv3.0 scores and the version(s) in which each vulnerability has been fixed.

CVE ID	CVSSv3.0 Score	Summary	ALEOS Fix Version(s)
CVE-2021-36727	7.5	AirLink ALEOS AT Command Password Brute-Force: The Telnet or SSH interface for AT commands is vulnerable to password brute-forcing. By default, ALEOS devices enable AT command access via Telnet on the LAN only, and use the random factory default password. The factory default password and strong user-defined passwords cannot be feasibly brute-forced due to limits on the login attempt rate. An attacker may be able to brute-force a weak user-defined password.	ALEOS4.15.0
CVE-2021-36728	7.2	AirLink ALEOS SMS Password Command Injection: An authenticated user can escalate privilege by configuring the SMS password.	ALEOS4.14.0, ALEOS4.9.6
CVE-2021-36729	4.7	AirLink ALEOS TLS Denial of service: It is possible for a user connected to AceManager over HTTPS to exhaust resources on the router.	ALEOS4.15.0
CVE-2021-36730	4.0	AirLink ALEOS AceManager Stack Buffer Overflows: Several stack buffer overflows exist in components of AceManager, allowing an authenticated user to cause internal processes to restart.	ALEOS4.15.0
CVE-2021-36731	2.7	AirLink ALEOS AceManager Resource Exhaustion: An authenticated user can cause AceManager to exhaust certain system resources, making it unavailable until the router is rebooted.	ALEOS4.15.0, ALEOS4.9.6
CVE-2021-36732	2.0	AirLink ALEOS SMS Password Logged: When the SMS password is changed, it is written to the logfile in plain text. The password may be inadvertently exposed if log files are shared.	ALEOS4.14.0
CVE-2021-36733	1.9	AirLink ALEOS AT Command Stack Buffer Overflow: A malformed AT command may cause an internal process to restart on GX450.	ALEOS4.9.6

Recommended Actions

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

CVE-2021-36727 AirLink ALEOS AT Command Password Brute-Force

If upgrade is not possible or you are running ALEOS 4.4.x or ALEOS 4.9.x, the following actions can mitigate this vulnerability:

- Ensure that any user-configured device and AT command passwords are strong and difficult to guess. Sufficiently strong, random passwords cannot be feasibly brute-forced. Where possible, use different passwords on different devices in your fleet.
- By default, ALEOS devices enable AT command access via Telnet on the LAN only. If you do not require AT command access on the LAN or WAN, you can fully disable access by setting "Telnet/SSH Access Policy" to "Disabled" under Services → AT (Telnet/SSH).

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/iot-device-security/security-bulletins/