Product Security Advisory: ALEOS Security Advisory

Sierra Wireless Advisory: SWI-PSA-2023-006

Date: 28 November 2023

Summary

Sierra Wireless was recently informed of eight security vulnerabilities in ALEOS, the operating system used in certain Sierra Wireless AirLink Routers, including the MP70, RV50x, RV55, LX40, LX60 ES450 and GX450. The vulnerabilities are present in ALEOS 4.16 and earlier versions and have been remediated in ALEOS 4.17 released in October 2023.

CVE ID	Description	CVSSv3.1
CVE-2023-40458	The ACEManager component of ALEOS 4.16 and earlier uses an open-source component which is vulnerable to an infinite loop condition, which could potentially allow a remote attacker to trigger a Denial of Service (DoS) condition for ACEManager without impairing other router functions. This condition is cleared by restarting the device.	7.5
CVE-2023-40459	The ACEManager component of ALEOS 4.16 and earlier does not adequately perform input sanitization during authentication, which could potentially result in a Denial of Service (DoS) condition for ACEManager without impairing other router functions. ACEManager recovers from the DoS condition by restarting within ten seconds of becoming unavailable.	7.5

CVE-2023-40460	The ACEManager component of ALEOS 4.16 and earlier does not validate uploaded file names and types, which could potentially allow an authenticated user to perform client-side script execution within ACEManager, altering the device functionality until the device is restarted.	7.1
CVE-2023-40461	The ACEManager component of ALEOS 4.16 and earlier allows an authenticated user with Administrator privileges to access a file upload field which does not fully validate the file name, creating a Stored Cross-Site Scripting condition.	8.1
CVE-2023-40462	The ACEManager component of ALEOS 4.16 and earlier does not perform input sanitization during authentication, which could potentially result in a Denial of Service (DoS) condition for ACEManager without impairing other router functions. ACEManager recovers from the DoS condition by restarting within ten seconds of becoming unavailable.	7.5
CVE-2023-40463	When configured in debugging mode by an authenticated user with administrative privileges, ALEOS 4.16 and earlier store the SHA512 hash of the common root password for that version in a directory accessible to a user with root privileges or equivalent access.	8.1
CVE-2023-40464	Several versions of ALEOS, including ALEOS 4.16.0, use a hardcoded SSL certificate and private key. An attacker with access to these items could potentially perform a man in the middle attack between the ACEManager client and ACEManager server.	8.1
CVE-2023-40465	Several versions of ALEOS, including ALEOS 4.16.0, include an open-source third-party component which can be exploited from the local area network, resulting in a Denial of Service condition for the captive	DoS

	portal. This vulnerability could potentially be exploited to trigger Remote Code Execution in the root context.	4.3 RCE 8.3

Affected Products

These vulnerabilties affect all AirLink routers running ALEOS software releases prior to version 4.9.9 (ES450, GX450) and prior to 4.17.0.12 (MP70, RV50x, RV55, LX40, LX60).

Recommended Actions

Upgrade to ALEOS 4.17.0.12 (MP70, RV50x, RV55, LX40, LX60) as soon as possible or ALEOS 4.9.9 (ES450, GX450). Pending upgrade, the following mitigations are recommended:

1. Always use strong, and ideally unique random credentials for your devices. ALEOS devices ship by default with unique random credentials.

2. Disable access to ACEManager on the WAN and make use of the Sierra Wireless Airlink Management System (ALMS) or an alternative device management platform for remote management of your ALEOS devices.

3. If you must leave ACEManager accessible via the WAN, restrict access using measures such as Private APN, VPN, or the ALEOS Trusted IP feature that restricts access to specific hosts.

4. Disable Debug Mode on AirLink devices when not being used for diagnostic purposes.

5. Sierra Wireless recommends that customers using devices which are no longer supported and not receiving the 4.17.0.12 or 4.9.9 updates refesh those devices with actively supported devices.

Credit

Sierra Wireless would like to thank Dr. Stanislav Dashevskyi of ForeScout for bringing these issues to our attention. We encourage anyone with a security concern related to Sierra Wireless products to please contact us at security@sierrawireless.com.

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/