December 8, 2023

Overall rating: High

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a Sierra Wireless AirLink vulnerability. The vulnerability affects AirLink ALEOS firmware, all versions prior to 4.9.9 and AirLink ALEOS firmware all versions prior to 4.17.0.

Technical Details

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. Additionally, 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. 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.

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. 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. 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.

Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in Sierra Wireless, Inc ALEOS 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.

Successful exploitation of these vulnerabilities could allow an attacker to perform remote code execution to take full control of the device, steal credentials through a cross site scripting attack, or crash the device being accessed through a denial-of-service attack.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-40458, CVE-2023-40459, CVE-2023-40460, CVE-2023-40461, CVE-2023-40462, CVE-2023-40463, CVE-2023-40464
- ICSA-23-341-06 Sierra Wireless AirLink with ALEOS firmware
- VRM Vulnerability Reports