Product Security Advisory: ALEOS Local Privilege Escalation and LAN-Side RPC Server Remote Code Execution

Sierra Wireless Advisory SWI-PSA-2020-005 (link to latest version)

Date of issue: September 17, 2020

Summary

Sierra Wireless has confirmed two security issues in ALEOS that could allow local privilege escalation and remote code execution.

The issues are present in the following AirLink products running all versions of ALEOS:

- LX40, LX60, MP70, MP70E, RV50, RV50X and RV55
- ES450 and GX450
- ES440, GX400, GX440 and LS300

Neither of these issues allows compromise of a gateway with default configuration.

Scope of Impact

ALEOS UpdateRebootMgr Service Privilege Escalation

An escalation to root is possible from a low-privilege process via the UpdateRebootMgr service in ALEOS 4.11 and later due to lack of input sanitization. In order to exploit this vulnerability, an attacker must first compromise another process running on the gateway. This vulnerability is not present in ALEOS 4.9.x or ALEOS 4.4.x.

CVE-2020-8781 has been assigned to this issue, with the title "ALEOS UpdateRebootMgr Service Privilege Escalation." Sierra Wireless has assigned a CVSSv3.0 score of 8.8 based on the vector CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H.

This issue will be fixed in ALEOS 4.14.0.

ALEOS LAN-Side RPC Server Remote Code Execution

A LAN-side unauthenticated RPC server was previously disclosed as CVE-2019-11855. In versions of ALEOS prior to 4.12.0, 4.9.5, or 4.4.9, enabling ALEOS Application Framework (AAF) would enable a Lua RPC server. This RPC server is designed to allow debugging on the gateway during application development. IOActive has demonstrated that this RPC server permits remote code execution when enabled.

CVE-2020-8782 has been assigned to this finding, with the title "ALEOS LAN-Side RPC Service Remote Code Execution." Sierra Wireless has assigned a CVSSv3.0 score of 8.1 based on the vector CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H.

In ALEOS versions 4.12.0, 4.9.5, 4.4.9, and newer, the RPC server is only enabled when the AAF user password is defined on the gateway. In ALEOS 4.14.0, 4.9.5, and 4.4.9, a warning message will appear in ACEmanager when the AAF user password is defined.

Recommended Actions

In current versions of ALEOS, the RPC server is enabled only when the AAF user password is defined. Sierra Wireless recommends that customers enable the AAF user only for devices that are being used for AAF development and debugging. The AAF user is not required for AAF applications to be deployed and run. Deployed devices must not have the AAF user password enabled.

Sierra Wireless recommends upgrading to the latest ALEOS version for your gateway. For devices running ALEOS 4.13, Sierra Wireless recommends upgrading to ALEOS 4.14.0 once it is available.

Credits

These vulnerabilities were discovered by Ruben Santamarta, Principal Security Consultant at IOActive and were published in the blog post here. For further information please visit https://ioactive.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/