Technical Bulletin: PPPD Vulnerabilities in AirLink Products

Sierra Wireless Advisory SWI-PSA-2020-001

Date of issue: Mar 5, 2020

Summary

Recently published research has identified a vulnerability in the Point-to-Point Protocol Daemon (PPPD) in ALEOS and MGOS. The following Common Vulnerability and Exposure (CVE) identifier has been assigned to this vulnerability:

CVE-2020-8597	eap.c in pppd in ppp 2.4.2 through 2.4.8 has an rhostname buffer overflow in the eap_request and eap_response functions.

Sierra Wireless would like to thank Ilja Van Sprundel of IOActive for discovering and responsibly reporting this issue, Paul Mackerras for creating the patch for pppd, and CERT for coordinating the response.

Scope of Impact

A logic flaw in the Point-to-Point Protocol Daemon (PPPD) may allow an unauthenticated attacker to inject arbitrary code to execute on the target system. The PPPD service can be impacted in both client and server modes.

On Sierra Wireless AirLink products, PPPD is not enabled by default on any interface. All optional interfaces implementing PPPD require either physical access or short-range wireless access.

Sierra Wireless has assigned a CVSSv3 score of 8.1 to these product vulnerabilities based on the vector CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H.

Affected Products

The following table lists the impacts of the vulnerability to each AirLink product, along with the firmware version that will include a fix.

Product	Impact	Fix Version	Target Release Date
LS300, GX400, GX440, ES440	Gateway acts as: PPP server for RS232 (Serial) PPP, if configured. PPP server for USB Serial PPP, if configured.	ALEOS 4.4.9	Apr 2020
GX450, ES450		ALEOS 4.9.5	May 2020
LX40, LX60, MP70, MP70E, RV50, RV50X, RV55		ALEOS 4.14	Oct 2020
OMG2000	Gateway acts as: PPP server for Bluetooth Dial-Up Networking (DUN), if configured; Bluetooth DUN connections also require a valid Bluetooth PIN. PPP server for Serial LAN client, if configured. (MG90 only) PPP client for Land Mobile Radio (LMR), if configured. PPP client for PPP adapter cards, if configured. (OMG2000 only)	MGOS 3.15.2	May 2020
MG90		MGOS 4.3.1	Sep 2020

Note that where the gateway acts as a PPP client, the peer to which it connects must be compromised or replaced in order to send a malicious packet. For example, where an MG90 is connected to a Land-Mobile Radio (LMR), an attacker must first compromise the LMR in order to have it send a malicious packet. Sierra Wireless evaluates the risk in PPP client mode as being lower than for PPP server mode.

Recommended Actions

Sierra Wireless recommends upgrading to the fix version for your gateway once it is released.

No mitigations are required unless one of the optional features listed in the table has been enabled on your gateway. If one of the optional features is enabled, the following measures should be taken until the gateway can be upgraded to the fix version:

- For enabled physical interfaces from the table where the gateway acts as a server, ensure that the device remains physically secure until the gateway can be patched.
- For Bluetooth DUN on MGOS devices, ensure that the Bluetooth PIN for the device is not shared.
- For any interfaces operating in PPP client mode, follow the manufacturer's recommendations in order to secure and update the PPP server device (such as the LMR).

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/