Sierra Wireless Security Advisory SWI-PSA-2018-005: CVE-2018-10251: Remote Code Execution Vulnerability

Release Date: April 30, 2018

Version: 1

Issue Description:

A vulnerability in some AirLink routers running older versions of firmware could allow an unauthenticated remote attacker to execute arbitrary code and gain full control of an affected system, including issuing commands with root privileges.

Sierra Wireless has released firmware updates that address this vulnerability.

Impact:

CVSS Severity (version 3.0):

CVSS v3 Base Score: 8.8
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

CVSS Version 3 Metrics:

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): Required
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

Workarounds/Mitigations:

Users can mitigate the potential for an exploit by following recommended security practices including, but not limited to:

1. Replace the router default password(s) with strong passwords.
2. Restrict remote access to your router through the use of private APNs, VPNs and firewall techniques such as Trusted IP.
3. Disable AceManager on all WAN interfaces (default configuration since ALEOS 4.5.1), if enabled.
4. Use physical security measures to prevent unauthorized access to local ports.

Affected Products:

This vulnerability affects only the following products running the specified firmware versions. Products not listed are not affected by this issue.

Product	Affected Version(s)
GX400, GX440, ES440, LS300	<4.4.7
GX450, ES450, RV50, RV50X, MP70, MP70E	<4.9.3

Solution:

Users should upgrade to firmware version 4.4.7 (GX400, GX440, ES440, LS300) or version 4.9.3 (GX450, ES450, RV50, MP70). It is always recommended that users keep their equipment updated to the latest firmware version.

Exploitation and Public Announcements

Sierra Wireless is aware of malicious use of this vulnerability. Customers operating any of the affected products should refer to the following technical bulletin for instructions on how to engage Sierra Wireless for assistance in remediating this issue:

https://source.sierrawireless.com/resources/airlink/software_reference_docs/technical-bulletin/swi-psa-2018-003-technical-bulletin-reaper/

Credits:

This issue was discovered during an investigation into malware infections of AirLink products.