Sierra Wireless Security Advisory SWI-PSA-2018-004: CVE-2017-15043: 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 authenticated remote attacker to execute arbitrary code and gain full control of an affected system, including issuing commands with *root* privileges.

This vulnerability is due to insufficient input validation on user-controlled input in an HTTP request to the targeted device. An attacker in possession of router login credentials could exploit this vulnerability by sending a crafted HTTP request to an affected system. A successful exploit could allow the attacker to execute arbitrary code as the root user and gain full control of the affected system.

Sierra Wireless has released firmware updates that address this vulnerability.

Impact:

CVSS Severity (version 3.0):

CVSS v3 Base Score: 8.0
Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

CVSS Version 3 Metrics:

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): Low
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.
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	<4.4.5
GX450, ES450, RV50, MP70	<4.9

Solution:

Users should upgrade to the latest available firmware versions for their products. As of the publication date of this bulletin those versions are:

- 4.4.7 for GX400, GX440, ES440, LS300
- 4.9.3 for GX450, ES450, RV50, MP70

Exploitation and Public Announcements

Sierra Wireless is aware of malicious use of this vulnerability and has engaged with the owners of known affected devices to assist with remediation.

Credits:

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