America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Archived Content

In an effort to keep CISA.gov current, the archive contains outdated information that may not reflect current policy or programs.

ICS ADVISORY

Sierra Wireless AirLink ALEOS (Update B)

Last Revised: April 23, 2020 **Alert Code:** ICSA-19-122-03

1. EXECUTIVE SUMMARY

- **CVSS v3 9.1**
- **ATTENTION:** Exploitable remotely/low skill level to exploit/public exploits are available
- **Vendor:** Sierra Wireless
- **Equipment:** AirLink ALEOS
- **Vulnerabilities:** OS Command Injection, Use of Hard-coded Credentials, Unrestricted Upload of File with Dangerous Type, Cross-site Scripting, Cross-site Request Forgery, Information Exposure, Missing Encryption of Sensitive Data

2. UPDATE INFORMATION

This updated advisory is a follow-up to the original advisory titled ICSA-19-122-03 Sierra Wireless AirLink ALEOS (Update A) that was published August 20, 2019, on the ICS webpage on us-cert.gov.

3. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow attackers to remotely execute code, discover user credentials, upload files, or discover file paths.

4. TECHNICAL DETAILS

4.1 AFFECTED PRODUCTS

Sierra Wireless reports the vulnerabilities affect the following AirLink ALEOS versions and products:

--------- Begin Update B Part 1 of 2 ---------

- LS300, GX400, GX440, and ES440: All versions prior to 4.4.9

--------- End Update B Part 1 of 2 ---------

- GX450 and ES450: All versions prior to 4.9.4
- MP70, MP70E, RV50, RV50X, LX40, and LX60: All versions prior to 4.12

4.2 VULNERABILITY OVERVIEW

4.2.1 IMPROPER NEUTRALIZATION OF SPECIAL ELEMENTS USED IN AN OS COMMAND ('OS COMMAND INJECTION') CWE-78

<https://cwe.mitre.org/data/definitions/78.html>

A specially crafted authenticated HTTP request can inject arbitrary commands, resulting in remote code execution.

CVE-2018-4061 has been assigned to this vulnerability. A CVSS v3 base score of 9.1 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:h/ui:n/s:c/c:h/i:h/a:h>).

4.2.2 USE OF HARD-CODED CREDENTIALS CWE-798

<https://cwe.mitre.org/data/definitions/798.html>

Activating SNMPD outside of the WebUI can cause the activation of the hard-coded credentials, resulting in the exposure of a privileged user. An attacker can activate SNMPD without any configuration changes to trigger this vulnerability.

CVE-2018-4062 has been assigned to this vulnerability. A CVSS v3 base score of 6.2 has been calculated; the CVSS vector string is (AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:L/A:H <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:h/pr:h/ui:n/s:u/c:h/i:l/a:h>).

4.2.3 UNRESTRICTED UPLOAD OF FILE WITH DANGEROUS TYPE CWE-434 <https://cwe.mitre.org/data/definitions/434.html>

A specially crafted authenticated HTTP request can upload a file, resulting in an executable, routable code upload to the web server.

CVE-2018-4063 has been assigned to this vulnerability. A CVSS v3 base score of 9.1 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:h/ui:n/s:c/c:h/i:h/a:h>).

4.2.4 IMPROPER NEUTRALIZATION OF INPUT DURING WEB PAGE GENERATION ('CROSS-SITE SCRIPTING') CWE-79

<https://cwe.mitre.org/data/definitions/79.html>

A specially crafted HTTP ping request can cause reflected JavaScript to be executed and run on the user's browser. An attacker can exploit this by convincing a user to click a link or embedded URL that redirects to the reflected cross-site scripting vulnerability.

CVE-2018-4065 has been assigned to this vulnerability. A CVSS v3 base score of 6.1 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:r/s:c/c:l/i:l/a:n>).

4.2.5 CROSS-SITE REQUEST FORGERY (CSRF) CWE-352

<https://cwe.mitre.org/data/definitions/352.html>

A specially crafted HTTP request can cause an authenticated user to perform privileged requests unknowingly, resulting in unauthenticated requests through an authenticated user. Triggering this vulnerability may allow an attacker access to authenticated pages via an authenticated user.

CVE-2018-4066 has been assigned to this vulnerability. A CVSS v3 base score of 6.8 has been calculated; the CVSS vector string is (AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:H <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:h/pr:n/ui:r/s:u/c:n/i:h/a:h>).

4.2.6 INFORMATION EXPOSURE CWE-200

<https://cwe.mitre.org/data/definitions/200.html>

A specially crafted authenticated HTTP request can cause an information leak, resulting in the disclosure of internal file paths.

CVE-2018-4067 has been assigned to this vulnerability. A CVSS v3 base score of 4.1 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:h/ui:n/s:c/c:l/i:n/a:n>).

4.2.7 MISSING ENCRYPTION OF SENSITIVE DATA CWE-311

<https://cwe.mitre.org/data/definitions/311.html>

The ACEManager authentication functionality is delivered in plaintext XML to the web server. An attacker can listen to network traffic upstream from the device, which may allow access to credentials.

CVE-2018-4069 has been assigned to this vulnerability. A CVSS v3 base score of 5.9 has been calculated; the CVSS vector string is (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:h/pr:n/ui:n/s:u/c:h/i:n/a:n>).

4.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Commercial Facilities, Communications, Emergency Services, Energy, Government Facilities, Transportation Systems, Water and Wastewater Systems
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** Canada

4.4 RESEARCHER

Carl Hurd and Jared Rittle of Cisco Talos reported these vulnerabilities to Sierra Wireless.

5. MITIGATIONS

--------- Begin Update B Part 2 of 2 ---------

Sierra Wireless recommends users upgrade to the latest version of ALEOS for the products and versions below. For upgrade assistance, contact an authorized AirLink reseller, Sierra Wireless sales, technical representative, or Sierra Wireless technical support.

- LS300, GX400, GX440, ES440: ALEOS 4.4.9
  - The ALEOS 4.4.9 Release Note <https://source.sierrawireless.com/resources/airlink/software_reference_docs/release-notes/aleos-4,-d-,4,-d-,9-release-notes/> is available (login required)
- GX450, ES450: ALEOS 4.9.4.p09
- MP70, MP70E, RV50, RV50X, LX40, LX60: ALEOS 4.12
  - The ALEOS 4.12.0 Release Note <https://source.sierrawireless.com/resources/airlink/software_reference_docs/release-notes/aleos-4,-d-,12,-d-,0-release-notes/> is available (login required)

--------- End Update B Part 2 of 2 ---------

Sierra Wireless recommends users follow the actions outlined below:

- Ensure a strong password is set for the user account. For guidance on password strength, Sierra Wireless recommends the “memorized secret authenticator” guidelines in NIST SP800-63B.
- If ALEOS Application Framework (AAF) is enabled, ensure a strong password is set for the AAF User account.
- If Telnet or SSH is enabled, ensure a strong password is set for the console account.

When connecting directly to ACEmanager:

- Use only HTTPS.
- Utilize an up-to-date, modern web browser with built-in CSS and CSRF protection, such as Chrome, Firefox, or Edge.

For more information, see the Sierra Wireless security advisory <https://source.sierrawireless.com/resources/airlink/software_reference_docs/technical-bulletin/sierra-wireless-technical-bulletin---swi-psa-2019-003/>.

The following SNORT rules will detect exploitation attempts. Note that additional rules may be released at a future date and current rules are subject to change pending additional vulnerability information. For the most current rule information, please refer to a Firepower Management Center or Snort.org.

Snort Rules: 48600, 48635, 48614 - 48621, 48747

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. <https://www.us-cert.gov/ics/alerts/ics-alert-10-301-01>
- Locate control system networks and remote devices behind firewalls and isolate them from the business network.
- When remote access is required, use secure methods, such as virtual private networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practice <https://www.us-cert.gov/ics/recommended-practices>s on the ICS webpage on us-cert.gov <https://www.us-cert.gov/>. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on us-cert.gov <https://www.us-cert.gov/ics> in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies

<https://www.us-cert.gov/sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to CISA for tracking and correlation against other incidents.

CISA also recommends users take the following measures to protect themselves from social engineering attacks:

- Do not click web links or open unsolicited attachments in email messages.
- Refer to Recognizing and Avoiding Email Scams <https://www.us-cert.gov/sites/default/files/publications/emailscams_0905.pdf> for more information on avoiding email scams.
- Refer to Avoiding Social Engineering and Phishing Attacks <https://www.us-cert.gov/ncas/tips/st04-014> for more information on social engineering attacks.

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Vendor

- Sierra Wireless

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov