Technical Bulletin: SSH Proxy

Sierra Wireless Advisory SWI-PSA-2019-004 (Link to latest version)

Date of issue: May 2, 2019

Updated: August 7, 2020

Applicable Products

AirLink® LS300, GX400, GX/ES440, GX/ES450, RV50, RV50X, MP70, MP70E, LX60 and LX40 gateways and routers that:

- Are directly reachable from the public internet, and
- Have SSH reachable over the WAN

Summary

The Sierra Wireless security team has received reports of AirLink devices with SSH remote access enabled acting as proxy servers for external parties. Further investigation of reported devices shows that attackers are using compromised usernames and passwords to gain authenticated access to SSH and use the service as a proxy.

Known impacts of this attack are:

- Affected devices are proxying external data, and as such, may incur higher data rates.
- External parties may be able to access ACEmanager and local LAN services, even if remote ACEmanager is not enabled.

All affected customers are advised to take immediate action as detailed in this bulletin.

Added 2020-08-07:

CVE-2019-11862 has been assigned to this issue, with the title "ALEOS SSH Service Allows Traffic Proxying." Sierra Wireless has assigned a CVSSv3 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.

The issue has been fixed in the following ALEOS versions: 4.12.0, 4.9.5, and 4.4.9.

Recommended Actions

Sierra Wireless advises customers to follow the recommended actions outlined below. If you require assistance performing these actions or have routers that are exhibiting suspicious behavior, please contact your authorized AirLink reseller and/or your Sierra Wireless sales or technical representative. Alternatively, you can also contact Sierra Wireless technical support for assistance.

1. If SSH remote access is not required, disable remote access:
   a. In ACEmanager, navigate to Services > Telnet/SSH
   b. Set 'Telnet/SSH Access Policy' to 'LAN' (default) or 'Disabled'.
2. If SSH remote access is required, change the user and sconsole password on all devices to a new secure value, even if the devices previously had a non-default password as the password may have been previously compromised.
   a. In ACEmanager, navigate to Admin > Change Password
   b. Select 'user' as the 'Username', enter a strong new password, and click 'Change Password'
   c. Select 'sconsole' as the 'Username', enter a strong new password, and click 'Change Password'

Added 2020-08-07:
Sierra Wireless recommends upgrading your gateway or router to the latest supported ALEOS version.

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/