Sierra Wireless Technical Bulletin: Malware Threat

Products: AirLink® Gateways running ALEOS 4.5.2 or older using default user or viewer password

Date of issue: 4 September 2017 (Updated 11 September 2017)

The Sierra Wireless security team has discovered a new malware threat targeting gateways running ALEOS 4.5.2 or older that are using default user or viewer passwords and are directly reachable from the public internet. We take such threats seriously and are actively working with law enforcement, network operators, channel partners and affected customers to address the malware threat and assist in remediation of affected gateways.

To date, we have only seen evidence of the malware affecting GX400 and GX440 gateways using default user or viewer passwords. However, we encourage all customers to follow the recommendations in this bulletin as best practice for all AirLink Gateways.

On an affected gateway, the malware will periodically contact a command and control server for instructions and potentially participate in a Distributed Denial of Service (DDoS) attack. Furthermore, in some deployments compromised gateways will no longer be able to boot. In this state, the gateway will display solid green power LED and reboot every 1-4 minutes.

All customers are advised to immediately follow the recommended actions detailed in this bulletin. If you require assistance performing these actions or have gateways that are no longer booting, please contact your authorized AirLink reseller and/or your Sierra Wireless sales or technical representative. Alternatively, you can contact Sierra Wireless technical support at https://www.sierrawireless.com/company/contact-us/

Recommended Actions

Sierra Wireless strongly recommends that customers operating gateways with ALEOS 4.5.2 or older that are using the default user or viewer password immediately perform the following actions:

1. To protect your gateway(s) from the malware: Ensure that strong, unique passwords are used for both the user and viewer accounts on the gateway:
    a. In ACEmanager or ALMS, navigate to **Admin > Change Password**
    b. Set a strong, unique password for both the **user** and **viewer** accounts.
2. To ensure the malware described in this bulletin is not present on your gateway(s): **Re-install your current firmware or, if possible, upgrade to the latest available firmware**. The following table details the most current firmware for all identified products:

Product	Most recent firmware version
LS300	4.4.4.p05
GX400	
GX/ES440	
GX/ES450	4.8.1
RV50	

Configuration changes and firmware updates can be performed on individual gateways using ACEmanager or on multiple gateways at the same time using AirLink Management Service (ALMS). ALMS is free for customers with up to 15 gateways. For more information please visit https://na.airvantage.net/accounts/signup?type=AVMS_AL.

Further Information

For further information and technical support, please contact your authorized AirLink reseller or Sierra Wireless representative. To contact Sierra Wireless, please visit https://www.sierrawireless.com/company/contact-us/.

For more information on product security and to sign up for security updates, please visit https://www.sierrawireless.com/company/security/