Sierra Wireless Technical Bulletin: IoTroop/Reaper Malware

Date of issue: 29 March 2018

Applicable Products

AirLink® Gateways that have ever been connected to the internet while using a default user or viewer password and while running the following firmware versions:

Model	Affected Firmware Version
LS300, GX400, GX/ES440	ALEOS 4.4.4 or older
GX/ES450, RV50, RV50X, MP70, MP70E	ALEOS 4.8.1 or older

Please note: this includes gateways that have been subsequently upgraded to 4.9.0, 4.9.1 or 4.4.5.

Summary

Sierra Wireless has observed IoTroop/Reaper infecting Airlink gateways running older firmware, using default user or viewer passwords and that are directly reachable from the public internet. We take such threats seriously and are actively working with network operators, channel partners and affected customers to address this threat and assist in remediation of affected gateways.

The malware is known to have the following impacts:

a) During installation of the malware, the gateway's user password will be stolen and sent to the malware's command and control server. This may allow the gateway to be re-infected if the malware is removed but the user password is not changed.

b) The malware will periodically contact a command and control server for instructions and potentially participate in a Distributed Denial of Service (DDoS) attack. This may result in significant unexpected data charges.

All customers are advised to immediately follow the recommended actions in this bulletin. Doing so will protect your gateways from this malware threat and clean the malware off the gateway if it is present.

Recommended Actions

Sierra Wireless strongly recommends that customers operating gateways that are directly reachable from the public internet **immediately perform these actions in the following order**:

1. To ensure the malware is not present on your gateway(s): **Upgrade to the firmware indicated in the following table as soon as it becomes available.**

Product	New Firmware version
LS300, GX400, GX/ES440	ALEOS 4.4.6 or later
GX/ES450, RV50, RV50X, MP70, MP70E	ALEOS 4.9.2 or later

2. After upgrading the gateway firmware, **immediately change the user password on all gateways to a new secure value, even if the gateway(s) previously had a non-default password**.
   a. In ACEmanager, navigate to *Admin > Change Password*
   b. If you are using AirLink Managerment Service (ALMS) follow the instructions here: https://doc.airvantage.net/alms/reference/monitor/howtos/remotelyChangeACEManagerPassword/

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 assistance performing these actions or for further information, 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/