Sierra Wireless Technical Bulletin: IoTroop/Reaper Malware Update

Date of issue: 20 April 2018

Updated: 3 May 2018 (version 2)

Applicable Products

AirLink® LS300, GX400, GX/ES440, GX/ES450, RV50, RV50X, MP70 and MP70E gateways and routers that are directly reachable from the public internet.

Summary

Further to the technical bulletin SWI-PSA-2018-002 issued on 29 March 2018, Sierra Wireless has determined that the IoTroop/Reaper malware is using two methods to infect AirLink gateways and routers connected to the public internet. The primary method of infection is through default or stolen passwords (SWI-PSA-2018-004/CVE-2017-15043). However, during further investigation by the incident response team, we have identified a previously unknown vulnerability (SWI-PSA-2018-005/CVE-2018-10251) that is also in use.

The malware is known to have the following impacts:

a) During installation of the malware, the gateway's user password may be stolen and sent to the malware's command and control server. This may allow the gateway to be re-infected later 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 wireless data charges.

All users with AirLink gateways and routers that are reachable from the public internet are advised to contact Sierra Wireless immediately for assistance.

Sierra Wireless Technical Support

1-877-552-3860 (free of charge)

6:00am – 5:00pm Pacific Time, Monday to Friday.

The technical support team will assist users to remove any malware that is present and perform one or more of the following protective steps:

1. Register devices in AirLink Management Service (ALMS) to provide secure remote management; ALMS will be provided free of charge for the duration of the remediation process.
2. Mitigate the vulnerability by performing one or more of the following actions:
    a. Upgrade your routers and gateways to ALEOS 4.9.3 (GX/ES450, RV50, MP70) or 4.4.7 (LS300, GX400 and GX/ES440) or later;
    b. Disable remote access to ACEmanager (https://source.sierrawireless.com/resources/airlink/forum_topics_and_questions/how-to-disable-remote-access-to-acemanager/);
    c. Enable Trusted IP/Friends List (https://source.sierrawireless.com/resources/airlink/forum_topics_and_questions/how-to-enable-trusted-ip-friends-list/)
3. Update the gateway User password (https://source.sierrawireless.com/resources/airlink/forum_topics_and_questions/how-to-change-gateway-passwords/)

To ensure the fastest possible resolution of this issue, Sierra Wireless recommends that users build a list of their router and gateway serial numbers and IMEIs prior to calling the technical support team. This information is located on the label on the bottom of the product.

Further Information

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