Sierra Wireless Technical Bulletin: Mirai Malware

Products: Sierra Wireless LS300, GX400, GX/ES440, GX/ES450 and RV50

Date of issue: 4 October 2016

Sierra Wireless has confirmed reports of the "Mirai" malware infecting AirLink gateways that are using the default ACEmanager password and are reachable from the public internet. The malware is able to gain access to the gateway by logging into ACEmanager with the default password and using the firmware update function to download and run a copy of itself.

Based on currently available information, once the malware is running on the gateway it deletes itself and resides only in memory. The malware will then proceed to scan for vulnerable devices and report its findings back to a command and control server. The command and control server may also instruct the malware to participate in a Distributed Denial of Service (DDoS) attack on specified targets.

Currently, the best known indicator of the malware's presence is abnormal traffic on TCP port 23 as it scans for vulnerable devices. Customers may also observe command and control traffic on TCP port 48101 and a large amount of outbound traffic if the infected gateway is participating in a DDoS attack.

Because the malware resides only in memory, rebooting the gateway will remove the infection. However, if the gateway continues to use the default ACEmanager password, it will likely become re-infected.

Devices attached to the gateway's local area network may also be vulnerable to infection by the Mirai malware. Please be aware that Sierra Wireless gateways have a number of features that make these devices remotely accessible. As a result, we strongly recommend following the best practices identified in the "Protecting the Local Area Network" section below to ensure that such devices are not inadvertently exposed.

Products covered by this bulletin

This bulletin applies to the following Sierra Wireless products: LS300, GX400, GX/ES440, GX/ES450 and RV50.

Recommended Actions

Protecting the gateway

Sierra Wireless strongly recommends that customers with the identified products perform the following steps on each gateway:

1. Reboot the gateway to eliminate any existing Mirai malware; and
2. Immediately change the ACEmanager password to a secure, unique value. The password can be changed by either:
    a. Logging into ACEmanager and navigating to **Admin** > **Change Password**; or
    b. Remotely changing the password using the AirLink Managerment Service (ALMS). Instructions can be found at: https://doc.airvantage.net/alms/reference/monitor/howtos/remotelyChangeACEManagerPassword/

If you have multiple gateways and do not currently subscribe to ALMS, you can sign up for a free 30-day trial by visiting https://na.airvantage.net/accounts/signup?type=AVMS_AL

Protecting the Local Area Network

In order to protect devices on the gateway's local area network from Mirai and other security threats, Sierra Wireless recommends the following best practices:

1. If you do not need remote access to TCP or UDP services on devices attached to the gateway, disable the following features: DMZ Host; Public Mode; and Port Forwarding.
2. If you need remote access to TCP or UDP services on devices attached to the gateway:

a. If the TCP or UDP ports are known ahead of time, use Port Forwarding to forward only the required ports. Disable DMZ Host and Public Mode.

b. If the ports are not known ahead of time, customers may use the DMZ Host functionality to forward all ports to a specified IP. Sierra Wireless strongly advises using Port Filtering to filter inbound traffic on ports that do not require remote access, especially ports 23 (telnet) and 22 (SSH).

c. If an attached device requires knowledge of the internet/public IP, customers may use one of the Public IP modes. Sierra Wireless strongly advises using Port Filtering to filter inbound traffic on ports that do not require remote access, especially ports 23 (telnet) and 22 (SSH).

3. Where possible, use Trusted IP (also known as IP Whitelist) to reject traffic from unknown sources.

Disabling DMZ Host

1. Navigate to **Security** > **Port Forwarding**
2. Set **DMZ Host Enabled** to ***Disable***

Disabling Public Mode

1. Navigate to **LAN** > **DHCP/Addressing**
2. Set **Host Connection Mode** to ***All Hosts Use Private IPs***

Disabling Port Forwarding

1. Navigate to **Security** > **Port Forwarding**
2. Set **Port Forwarding** to ***Disable***

Using Trusted IP

1. Navigate to **Security** > **Trusted IPs – Inbound (Friends)**
2. Set **Inbound Trusted IP (Friends List) Mode** to ***Enable***
3. Set **Non-Friends Port Forwarding** to ***Disable***
4. Under **Inbound Trusted IP List** or **Inbound Trusted IP Range** click **Add More** and add IP addresses or IP ranges as required.

Adding an inbound port filter

1. Navigate to **Security** > **Port Filtering – Inbound**
2. Set **Inbound Port Filtering Mode** to ***Blocked Ports*** or ***Allowed Ports***
3. Click **Add More** and add port ranges as required.

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/