Sierra Wireless Technical Bulletin: Mirai

Products: Sierra Wireless AirLink® Gateways

Date of issue: 27 September 2016

Sierra Wireless has received reports of increased data traffic, consistent with infection by the "Mirai" Linux Trojan, at multiple customer sites. We take such reports seriously and are actively working with affected customers to determine the source of the suspicious traffic.

To best safeguard your network from the Mirai Trojan, we strongly recommend that you update your network settings and configuration as indicated below. We continue to investigate the specific customer issues and will provide further information and recommendations as warranted.

Products covered by this bulletin

This bulletin applies to the following products: Raven XE/XT; LS300; GX400; GX440; GX450; ES450; RV50; and MP70.

Recommended Actions

In order to ensure that network devices are not vulnerable to infection by Mirai, and other similar threats, Sierra Wireless recommends that all customers immediately perform the following actions:

1. Ensure that strong, unique passwords are used on all network devices. AirLink gateway passwords 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).
2. Where possible, use Trusted IP (also known as IP Whitelist) to reject traffic from unknown sources.
3. If devices attached to the gateway do not need to access remote telnet or SSH services, configure an outbound port filter for ports 23 (telnet) and 22 (SSH).

4. If you do not need remote access to TCP or UDP services on devices attached to the gateway, Sierra Wireless strongly recommends disabling the following features: DMZ Host; Public Mode; and Port Forwarding.
5. 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).

The configuration changes identified above can be made individually using ACEmanager or on multiple gateways at the same time using AirLink Management Service (ALMS). If you have multiple gateways and do not currently subscribe to ALMS, it is free to try for 30 days.

Please note that, when using ACEmanager to make configuration changes, you must click **Apply** before moving to the next page or any changes will be cancelled. When all configuration changes are complete, you must reboot the gateway in order for the changes to take effect.

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 outbound port filter for ports 22 (ssh) and 23 (telnet)

1. Navigate to **Security** > **Port Filtering – Outbound**
2. Set **Outbound Port Filtering Mode** to **Blocked Ports**
3. Click **Add More** and set **Start Port** to ***22*** and **End Port** to ***23***

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/