Sierra Wireless FAQ: Malware Threat

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

Date of issue: 11 September 2017

1. How would I know if we have been infected?

    a. The most reliable indicator of infection is a request to https://api.telegram.org every two minutes. If needed, customers can check for the presence of the malware by contacting Sierra Wireless support or by using the following procedure:

        i. Save the following string to "filter.txt":
        tcpdump -vvnnXXi wwan0 port 443 and net 149.154.167.0/24

        ii. Log in to ACEmanager and navigate to Admin > Advanced

        iii. Click "IP Logging"

        iv. Click "Browse" and select "filter.txt"

        v. Click Upload File

        vi. Click Start

        vii. If the number of packets captured is greater than zero after approximately 5 minutes, the presence of malware is likely.

2. Is there an abnormal spike in data usage when the malware has infected the gateway?

    a. An increase in data usage is expected. The increase depends on how long the malware has been present and whether it is participating in a DDoS attack.

3. If these devices have been infected do they need to be changed out?

    a. The malware can be removed by re-installing the current firmware or, if possible, by upgrading to the latest available firmware. If the gateway is non-functional and displaying a solid green power LED only and rebooting every 1-4 minutes it will need to be returned to Sierra Wireless for repair using the RMA process.

4. Would we have to worry about infected devices attacking our internal network or any other device on the LAN?

    a. Based on currently available information, it does not appear that the malware is self-propagating or capable of autonomously attacking devices on the LAN or internal network.

5. If I don't do anything, what's my risk?

    a. If your gateway is using a default user or viewer password and ACEmanager is reachable from the public internet, it may become infected with the malware. This could result in your gateway participating in a distributed denial of service (DDoS) attack which will generate a large amount of traffic over your mobile network connection. This will reduce the bandwidth available for your intended application(s) and likely result in a larger than expected data bill from your mobile network provider. In some cases, your gateway will become unable to boot and require RMA.

6. What is a Distributed Denial of Service (DDoS) attack? How does that affect me?

    a. A DDoS attack is when multiple internet devices start sending a continuous stream of data to a target site. The target site's internet connection is overwhelmed by the incoming traffic, effectively forcing it offline. This can result in important services such as Email becoming unavailable while the DDoS attack continues. Because the traffic is being generated by multiple devices, it is difficult to filter it out before it reaches the target site.

7. How is the malware finding Sierra Wireless gateways?

    a. The malware author is most likely scanning for devices on the internet that are listening on the default ACEmanager ports (9191 and 9443).

8. Is this something that will affect all my Sierra Wireless gateways?

    a. Based on the information currently available, the malware is only able to infect ALEOS-based gateways running software prior to version 4.6.0 that are using the default user or viewer password and reachable from the public internet. This includes the LS300, GX400, GX440 and ES440. GX450, ES450 and RV50 gateways that have not been updated to the latest firmware may also be affected. The malware does not appear to be able to infect other Sierra Wireless products.

9. How do I get this malware off my gateway?

    a. Re-install your current firmware or, if possible, upgrade to the latest available firmware.

10. How do I change the user and viewer passwords in AceManager?

    a. Log in to ACEmanager and navigate to **Admin** > **Change Password**; Be sure to change both the user and viewer passwords.

11. How do I get AirLink Management Service? How much will it cost me?

    a. ALMS is free for customers with up to 15 gateways. For more information please visit https://na.airvantage.net/accounts/signup?type=AVMS_AL.

12. How do I change the password in ALMS?

    a. Securely updating the passwords for multiple gateways takes some planning. Directions can be found at: https://doc.airvantage.net/alms/reference/monitor/howtos/remotelyChangeACEManagerPassword/

13. This would appear to be a risk only to devices deployed on public IP and not for devices on private networks.

    a. Based on currently available information, gateways that are not reachable from the public internet are not vulnerable to infection.

14. What practices does Sierra Wireless follow regarding the use of default passwords?

    a. To assist customers in protecting their gateway(s) and attached networks, Sierra Wireless makes continuous security enhancements to ALEOS in accordance with industry best practices. Recent changes have included:

        i. From ALEOS 4.5.0 onwards, remote access to ACEmanager is disabled by default;

        ii. From ALEOS 4.6.0 onwards, firmware images are cryptographically authenticated to ensure they originate from Sierra Wireless; and

        iii. From ALEOS 4.7.0 onwards, ACEmanager will notify users when the gateway is using the default password.

    b. In addition to these enhancements, Sierra Wireless is planning to migrate to a unique default password per device on the future products.