Product Security Advisory: AirLink Connection Manager (ACM) Security Advisory

Sierra Wireless Advisory: SWI-PSA-2023-005 (link to latest version)

Date August 10, 2023

Summary

Sierra Wireless has recently received reports of malicious actors attempting to compromise ACM instances that are deployed insecurely with exposed SSH and using the default administrative credentials. Sierra Wireless security guidance for the configuration of ACM instances strongly recommends changing the administrative credentials prior to operational deployment and limiting the exposure of SSH to secure management networks only.

As the frequency of compromise or compromise attempts appears to be increasing, Sierra Wireless strongly recommends that all customers review their ACM configuration and logs, and contact Sierra Wireless support if you have questions.

Affected Products

All versions of ACM may be vulnerable if they are deployed with SSH accessible from an insecure network such as the public Internet and are using insecure credentials, including default, weak, or publically known credentials.

Scope of Impact

If an attacker is able to connect to an ACM instance and authenticate they will gain full administrative control of the instance, allowing them to modify the configuration or access any secrets stored on the device.

Recommended Actions

Sierra Wireless recommends the following actions to secure your ACM instances:

- Ensure the administrative password, along with all other passwords, are changed from the defaults. All passwords should comply with accepted recommendations for strong passwords, such as those provided by Microsoft. For more information on how to change the ACM password please see the knowledge base article here.

- Set external firewall rules to prevent access to SSH from insecure or untrusted networks such as the public Internet, preventing untrusted connections.

- Monitor ACM and firewall logs for unauthorized access attempts from unknown sources and implement appropriate rules to block such attempts.

For advice on how to maintain a strong security posture for your ACM instance or if you have any questions regarding this advisory, please contact Sierra Wireless support personnel using the information provided at the end of this bulletin.

Support Contact Information

Sierra Wireless Technical Support is available by phone or web portal from 6:00 to 17:00 PST, Monday to Friday.

Phone (Toll-Free): 1-877-687-7795

Web: https://www.sierrawireless.com/support/community-portal/

Security Bulletins

To see the latest security updates from Sierra Wireless, please visit:

https://www.sierrawireless.com/company/security/