Product Security Advisory: Apache Log4j - CVE-2021-44228

Sierra Wireless Advisory: SWI-PSA-2021-007 (link to latest version)

Issued: December 14, 2021 1:15pm PST

Summary

The Sierra Wireless security team is conducting a comprehensive review to determine the impact of CVE-2021-44228 on our products and services.

> CVE-2021-44228: a remote code execution vulnerability in Apache Log4j. It is remotely exploitable without authentication, i.e., may be exploited over a network without the need for a username and password. https://nvd.nist.gov/vuln/detail/CVE-2021-44228

At this point in time, we have identified that our AM/AMM servers include a version of log4j identified in the CVE.

Due to the critical nature of this vulnerability and out of an abundance of caution, we have decided to take the action to temporarily suspend access to our Hosted AMM servers to reduce the impact of this vulnerability.

Affected Products and Services

On-premises AM/AMM Product: We are recommending that all customers with on-premises AM/AMM servers that have access to the public internet temporarily disable those servers until a remediation patch can be applied. Sierra Wireless is actively working on documenting a patching process that will allow on-premises customers to quickly patch their systems and return them to normal operation. We expect to be able to provide these details to you within the next 24-48 hours. Please contact Technical Support at the details set out below for further information.

Hosted AMM Services: Out of an abundance of caution, Sierra Wireless is in the process of temporarily suspending access to our Hosted AMM servers to reduce the impact of this issue, while we complete the required security patches. Once our full security assessment process is complete and the servers have been updated, services will be returned to a normal operational state and further communication will be provided. Hosted AMM customers can refer to https://status.sierrawireless.com/ for updates on our remediation efforts.

Scope of Impact

Vulnerable servers may be triggered to download and execute malware.

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/