TRIPP·LITE Powering and Connecting Your World

KNOWLEDGE BASE ARTICLE

2/15/2022

## Are Tripp Lite products are affected by the Log4j2 vulnerability?

A remote code execution vulnerability was recently discovered in Apache Log4j2 -- a Java library for logging error messages in applications. Reported as CVE-2021-44228, it affects Log4j versions up to and including 2.14.1 (excluding security release 2.12.2).

Log4j is commonly used by software solution providers, including Tripp Lite. The following list identifies the exposure of Tripp Lite products to this vulnerability and any corrective actions being undertaken.

**LX Platform devices** do not use log4j. This includes **WEBCARDLX**, **WEBCARDLXMINI**, **SRCOOLNETLX**, **SRCOOLNET2LX** and devices with pre-installed or embedded **WEBCARDLX** interfaces. **NOT AFFECTED**

**SNMPWEBCARD, SRCOOLNET, SRCOOLNET2** and devices with pre-installed or embedded **SNMPWEBCARD** interfaces do not use log4j. **NOT AFFECTED**

**TLNETCARD and associated software** do not use log4j. **NOT AFFECTED**

**PowerAlert Local (PAL)**
**PowerAlert Network Shutdown Agent (PANSA)**
**PowerAlert Network Management System (PANMS)**

> Some versions of these applications use log4j v1 which is **NOT AFFECTED** by the CVE-2021-44228 vulnerability. Tripp Lite is currently determining whether these applications are susceptible to a different, less severe vulnerability: CVE-2021-4104

**PowerAlert Element Manager (PAEM)**: Release 1.0.0 uses log4j version 2.11.2, making it **AFFECTED**.

Tripp Lite has issued **PAEM 1.0.2** which contains a patched version of Log4j2. This new version can be downloaded from the Tripp Lite website at the following URL:

https://assets.tripplite.com/firmware/paem-1.0.2.6.zip

ALTERNATE SOLUTIONS

In lieu of the PAEM 1.0.2 upgrade, PAEM 1.0.0 users can take the following actions to reduce exploit risk:

- Set the LOG4J_FORMAT_MSG_NO_LOOKUPS=”true” environment variable
  *Refer to: https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-cve-2021-44228-apache-log4j2/*

- Restricting access to only the machine on which PAEM is installed – disallow remote access to PAEM.