Systemware's Response to
CVE-2021-44832 Apache Log4j 2

systemware

Published on: 2021 Dec 29

Summary
Systemware continues our analysis of the remote code execution vulnerability (CVE-2021-44832) related to Apache Log4j2 (a logging tool used in many Java-based applications) disclosed on 28 Dec 2021. This vulnerability affects Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) if a JDBC appender is in use with a data source referencing a JNDI URI. By default Systemware does not provide configuration for a JDBC appender.

Any release of Systemware software prior to Version 7 is not impacted.

Solution
All current releases of Systemware Content Cloud Version 7 are now being remediated.

To address this vulnerability, Systemware updated our code from using log4j 2.17.0 to now use log4j 2.17.1. We updated our code on Tuesday, December 28, and will test these new builds this week.

If a customer uses a JDBC appender with a data source referencing a JNDI URI know that in 2.17.1 the property to enable JNDI has been renamed from 'log4j2.enableJndi' to three separate properties: log4j2.enableJndiLookup, log4j2.enableJndiJms, and log4j2.enableJndiContextSelector.

For any customer currently running Content Cloud Version 7.*, please contact technical support via phone, (972) 239-2803, or email and provide your current release levels for Cloud Manager, Content Integrator, Content Server DS, and Content Store. We will provide an updated build that is not subject to this vulnerability.

Mitigation

Systemware recommends an upgrade to the latest version of Content Cloud dated on or after December 29, 2021.

This is an immediate remediation.