Systemware's Response to
CVE-2021-45046 Apache Log4j 2

systemware

Published on: 2021 Dec 15

Summary
Systemware continues our analysis of the remote code execution vulnerability (CVE-2021-45046) related to Apache Log4j2 (a logging tool used in many Java-based applications) disclosed on 14 Dec 2021. This vulnerability affects Apache Log4j2 version 2.15.0.

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

Solution

All current releases of Systemware Content Cloud Version 7 have been remediated.

To address this vulnerability, Systemware updated our code from using log4j 2.15.0 to now use log4j 2.16.0. Current release levels are now available.

For any customer currently running Content Cloud Version 7.*, please contact technical support via phone, (972) 239-2803, or email (techsupport@systemware.com) 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

A. Edit the content cloud startup scripts as follows:

Add this line: export LOG4J_FORMAT_MSG_NO_LOOKUPS=true as the first line after the lines with the "#" end -- usually the 5th line.

Do this to each of the of the following scripts, depending on the product(s) installed:

1. Cloud Manager:
   a. /opt/systemware/cloud-cm/control

2. Content Integrator (2 locations)
   a. /opt/systemware/cloud-ci/control
   b. /opt/systemware/cloud-ci/cloudnode/ci/control

3. Content Server
   a. /opt/systemware/cloud-csd/control

4. Content Store
   a. /opt/systemware/cloud-cst/control

B. Restart the product.

This is an immediate remediation, a more permanent fix (with an upgrade of log4j2 2.16.0) will be or is already available in a patch release. You may also refer to the vulnerability page for other system mitigations. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046