Agilent Public Vulnerability Disclosure for CVE-2021-44228

Vulnerability Title: **Log4Shell: Remote Code Execution via Log4j2**

Vulnerability ID: CVE-2021-44228

Date of Discovery: 12/21/2021

Date of Disclosure: 05/15/2024

Agilent Product Impacted

Please direct any requests to CITSIRT@Agilent.com There will also be updated entries on the Agilent Community pages for customers to view with links the details from the product teams.

We were aware of the zero-day Log4J Vulnerability that was announced. Agilent is actively assessing our products and environment to identify any potential exposure from Log4J and to take steps to remediate if applicable.

We have determined that this vulnerability exists in the following products and steps are being taken to provide remediation information to customers.

Update:

SLIMS product (versions 6.6 and 6.7) – Customers informed and patches released for customers that have these versions installed.

Some OpenLab products including OpenLab Server, ECM XT, CDS Workstation Plus, and ChemStation Secure Workstation. Software updates and patches have been released to licensed customers.

Cary UV Workstation Plus - Versions 1.1 & 1.2: Software updates and patches have been released to licensed customers.

The following workstation Software versions are not vulnerable to unauthenticated attack and would require an attacker with local access and privileges to potentially exploit:

VWorks Plus – Versions 14.0.0. 14.0.1, 14.1.0

Our review and assessment related to Log4j is ongoing. We will notify our customers who have installed impacted products as we become aware of those products. Thank you for your patience.

Vulnerability Summary

The CVE-2021-44228 vulnerability, also known as 'Log4Shell,' affects Apache Log4j2 versions 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1). JNDI features used in configuration, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI-related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. Starting from version 2.16.0, this functionality has been

completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

Severity: Critical (CVSS v3.1 Base Score: 10.0)

Exploitability: High (CVSS v3.1 Exploit Code Maturity: High)

Agilent Response and Recommended Actions

Agilent Hosted SLIMS / SLIMS Cloud: the vulnerability is mitigated by the following factor:

- **SLIMS product (versions 6.6 and 6.7)** – Customers informed and patches released for customers that have these versions installed.

Agilent Software: the vulnerability is mitigated by the following factor:

- Some OpenLab products including **OpenLab Server, ECM XT, CDS Workstation Plus, and ChemStation Secure Workstation**. Software updates and patches have been released to licensed customers.
- **Cary UV Workstation Plus - Versions 1.1 & 1.2**. Software updates and patches have been released to licensed customers.
- **Vulnerability Remediation:** Agilent has upgraded its container base image to include the Apache Log4j2 fixes, so all most recent SLIMS (Cloud container) patch versions make use of these up-to-date packages. **Summary Actions Taken**
    - We have identified that some of our container images include Apache Log4j2, which is affected by the CVE-2021-44228 vulnerability.
    - We have updated the base image and the latest releases with a patched version and running instances were hotfixed.

References:

- Apache Log4j Vulnerability Guidance
- https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
- Microsoft Defender for Cloud blog post
- https://www.hhs.gov/vulnerability-disclosure-policy/index.html
- FDA guidance document on Postmarket Management of Cybersecurity in Medical Devices