Xylem Product Security Advisory

Third Party - Apache Log4j Vulnerabilities (v4.0)

December 15, 2021 (May 18, 2022)

Overview

Multiple vulnerabilities were released by the Apache Software Foundation which affect the Apache Log4j software library.

At this time, there is no evidence that these vulnerabilities have been exploited in the Xylem ecosystem. Xylem is in the process of delivering updated or remediated software to affected customers. The status of the affected software is listed within this advisory below.

Vulnerability Details

CVE ID: **CVE-2021-44228** (CVSS Score: 10.0 – Critical)

According to the Apache Software Foundation advisory, the vulnerability could allow for unauthenticated remote code execution and allow an attacker to execute code on vulnerable systems.

CVE ID: **CVE-2021-45046** (CVSS Score: 9.0 – Critical)

According to the Apache Software Foundation advisory, the vulnerability could allow for remote code execution in some environments and local code execution in all environments.

CVE ID: **CVE-2021-45105** (CVSS Score: 5.9 – Medium)

According to the Apache Software Foundation advisory, the vulnerability could allow for a denial-of-service (DOS) attack.

CVE ID: **CVE-2021-44832** (CVSS Score: 6.6 – Medium)

According to the Apache Software Foundation advisory, the vulnerability could allow for a remote code execution attack on vulnerable systems.

Based on Xylem's assessment, the risk of exploitation in Xylem's environment is minimized due to use of multi-layered security controls.

Patching of affected systems and implementation of additional mitigations are currently underway as listed in the table on the next page.

Affected Products

Xylem is currently investigating affected products and will update this table as more information becomes available.

Affected Products & Versions	Status
Aquatalk	Remediated
Avensor	Remediated
Sensus Analytics	Remediated
Sensus Automation Control	Remediated
Sensus Cathodic Protection (Sentry Point) • 4.9 and 4.10	Remediated
Sensus FieldLogic LogServer	Remediated
Sensus Lighting Control (Vantage Point)	Remediated
Sensus NetMetrics	Remediated
Sensus RNI *SaaS* • 4.7 through 4.10 • 4.4 through 4.6 • 4.2 *On Premise* • 4.7 through 4.10 • 4.4 through 4.6 • 4.2	*SaaS* Remediated for each affected version. *On Premise* Remediated software has been delivered to on-prem customers for each affected version.
Sensus SCS	Remediated
Smart Irrigation	Not impacted after further investigation.
Water Loss Management (Visenti)	Remediated
Xylem Cloud	Remediated
Xylem Edge Gateway (xGW)	Remediated

*Xylem products not listed in the above table are not impacted.

Security Recommendations

In alignment with CISA's guidance, Xylem strongly recommends affected organizations take the following actions:

- Upgrade to Log4j version 2.17.1
- Enumerate external-facing devices that have Log4j
- Continuously monitor for abnormal or unauthorized behavior on these devices
- Utilize a web application firewall (WAF) or other protection mechanisms to reduce risk

References

- CVE - https://nvd.nist.gov/vuln/detail/CVE-2021-44228
- CVE - https://nvd.nist.gov/vuln/detail/CVE-2021-45046
- CVE - https://nvd.nist.gov/vuln/detail/CVE-2021-45105
- CVE - https://nvd.nist.gov/vuln/detail/CVE-2021-44832
- Apache Log4j Security Page: https://logging.apache.org/log4j/2.x/security
- CISA Log4j Guidance: https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

Contact Information

For any questions related to this Xylem Product Security Advisory, please contact product.security@xylem.com.

Revision History	
Version	**Updates**
1.0	Initial draft
2.0	Added details for CVE-2021-45046 & CVE-2021-45105 and updated the remediation status for products.
3.0	Added details for CVE-2021-44832 and updated remediation status for products.
4.0	Updated remediation status for products.

Disclaimer

This document is provided on an as-is basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability or fitness for a particular use. Use of the information in this document or materials linked from this document is at your own risk. Xylem reserves the right the change or update this document any time.