

Xylem Product Security Advisory

Third Party - Apache Log4j Vulnerabilities (v2.0)

December 15, 2021 (December 20, 2021)

Overview

A vulnerability, known as Log4Shell (CVE-2021-44228), was released by the Apache Software Foundation which affects the Apache Log4j software library. This vulnerability impacts Apache Log4j versions 2.0-beta9 to 2.14.1, which is used in some of Xylem's products.

<December 20 Update>

CVE-2021-45046 was released by the Apache Software Foundation to address CVE-2021-44228 in Apache Log4j 2.15.0. This vulnerability impacts Apache Log4j versions 2.0-beta9 to 2.15.0.

CVE-2021-45105 was released by the Apache Software Foundation to address to address an additional denial-of-service (DOS) vulnerability impacting the latest log4j release 2.16.0. This vulnerability impacts Apache Log4j versions 2.0-alpha1 to 2.16.0.

<End Update>

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.

<December 20 Update>

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: 7.5 – High)

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

<End Update>

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, including the status for CVE-2021-45105.

Affected Products and Versions	Status CVE-2021-42288	Status CVE-2021-45046
Aquataalk	Patching complete	Patching complete
Avensor	Patching complete	Patching in process
Sensus Analytics	Patching complete	Patching complete
Sensus Automation Control	Configuration change complete	Patching in process
Sensus Cathodic Protection	Mitigation in process	Mitigation in process
Sensus FieldLogic LogServer	Patching complete	Patching complete
Sensus Lighting Control	Patching in process	Patching in process
Sensus NetMetrics	Configuration change complete	Patching in process
Sensus RNI <i>SaaS</i> 4.7 through 4.10 4.4 through 4.6 4.2 <i>On Prem</i> 4.7 through 4.10 4.4 through 4.6 4.2	- Configuration change complete - Patching in process - Patching in process - Mitigation in process - Patching in process - Patching in process	- Patching in process - Patching in process - Patching in process - Mitigation in process - Patching in process - Patching in process
Sensus SCS	Patching complete	Patching complete
Smart Irrigation	Remediation in process	Patching in process
Water Loss Management (Visenti)	Configuration change complete	Patching in process
Xylem Cloud	Patching complete	Patching complete
Xylem Edge Gateway (xGW)	Patching in process	Patching in process

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 2.17.0
- 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>
- 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 additional vulnerabilities CVE-2021-45046 & CVE-2021-45105 and updated the 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 on the document or materials linked from the document is at your own risk. Xylem reserves the right the change or update this document any time.