Document ID PN1579
Published Date 12/13/2021

Summary

Log4Shell Vulnerability Notice

Revision History

Revision Number

1.0

Revision History

Version 1.0 – 12/21/2021

Executive Summary

On December 9, 2021, a vulnerability was announced named “Log4Shell” by researchers. This vulnerability allows for remote code execution by exploiting the Java Logging Library log4j2.

Rockwell Automation is aware of this vulnerability and of how it could, if exploited, potentially impact our customers’ environments. Rockwell Automation is diligently working through the process of evaluation on how the mitigation techniques will impact the functionality and performance of the Rockwell Automation hardware, software, and pre-engineered products and solutions that incorporate this software. Rockwell Automation will continue to provide updated information as soon as reliable internal tests are completed.

Affected Products

Rockwell Automation is currently investigating its product portfolio to identify which of its products may be directly affected by the "Log4Shell" vulnerability. Rockwell Automation will continue to monitor this situation and will update this advisory if necessary. Our preliminary

investigation has indicated that the following Rockwell Automation products are affected, but mitigation techniques have already been put into place and the vulnerability is no longer a threat to Rockwell Automation customers.

- Plex (A Rockwell Automation Company) Industrial Internet of Things
- Fiix (A Rockwell Automation Company) CMMS core V5

The Plex Industrial Internet of Things product was affected by the vulnerability, but the proper mitigation technique has been put into place and it is no longer affected. A patch will be released on Monday to upgrade the product to Log4j2 version 2.15 which is not susceptible to the vulnerability.

The Fiix Computerized Maintenance Management Software core V5 SaaS was affected but has been patched to Log4j2 version 2.15 and is no longer susceptible to the vulnerability.

Vulnerability Details

CVE-2021-44228: Apache Log4j2 JNDI features do not protect against attacker-controlled LDAP and other JNDI related endpoints

Apache Log4j2 <=2.14.1 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 log4j2 2.15.0, this behavior has been disabled by default.

CVSS v3.1 Base Score: 10/10 [Critical]

CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Risk Mitigation & User Action

Vulnerability	Suggested Actions
CVE-2021-44228	**Plex Industrial IoT:** No user action needed as the product has already had the mitigation applied and it is no longer affected. In addition, a patch will be released 12/13/21 patching Log4j2 to version 2.15. **Fiix CMMS core V5:** No user action needed as the product has been updated to Log4j2 versions 2.15.

General Security Guidelines

Refer to the Industrial Network Architectures Page for comprehensive information about implementing validated architectures designed to complement security solutions.

Refer to the Industrial Security Services website for information on security services from Rockwell Automation to assess, protect, detect, respond and recover from incidents. These services include assessments, designs, implementations, industrial anomaly detection, patch management, and remote infrastructure monitoring and administration.

We also recommend concerned customers continue to monitor this advisory by subscribing to updates on the Security Advisory Index for Rockwell Automation, located in PN1345 – Industrial Security Advisory Index.

Rockwell Automation remains committed to making security enhancements to our systems in the future. For more information and for assistance with assessing the state of security of your existing control system, including improving your system-level security when using Rockwell Automation and other vendor controls products, you can visit the Rockwell Automation Security Solutions website .

If you have questions regarding this notice, please send an email to our product security inbox at: secure@ra.rockwell.com.

General Mitigations

- Use trusted software, software patches, antivirus/antimalware programs and interact only with trusted websites and attachments.
- Minimize network exposure for all control system devices and/or systems and confirm that they are not accessible from the Internet. For further information about the risks of unprotected Internet accessible control systems, please see PN715 - Advisory on web search tools that identify ICS devices and systems connected to the Internet
- Locate control system networks and devices behind firewalls and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

Additional Links

- NVD - CVE-2021-44228 (nist.gov)
- Log4j – Apache Log4j Security Vulnerabilities
- PN1354 - Industrial Security Advisory Index
- Deploying Industrial Firewalls within a CPwE Architecture Design and Implementation Guide