Security Advisory 12142021-002

CVE-2021-44228
CVE-2021-4104
CVE-2021-45046

Initial Publication Date: December 14, 2021

Vulnerability Details:

Vulnerability Note VU#930724

- Apache Log4j allows insecure JNDI lookups that could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the vulnerable Java application using Log4j.
- CISA has published Apache Log4j Vulnerability Guidance and provides a Software List.

CVE-2021-44228

- Apache Log4j2 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. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), 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.
- CVVS Version 3.X Score: 10.0 – Critical

CVE-2021-4104

- JMSAppender in Log4j 1.2 is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-44228. Note this issue only affects Log4j 1.2 when specifically configured to use JMSAppender, which is not the default. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.
- CVVS Version 3.X Score: 7.5 – High

CVE-2021-45046

- It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments. Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for message lookup patterns and disabling JNDI functionality by default.
- CVVS Version 3.X Score: 9.0 – Critical

Summary
The bug, dubbed Log4Shell or LogJam, is an unauthenticated RCE vulnerability allowing complete system takeover on systems with Log4j 2.0-beta9 up to 2.14.1.

After evaluation of all Multi-Tech products and services, it is determined Multi-Tech does not use the Log4j package in any of its products and services and are not affected by the log4j-vulnerability.

Customer Action Plan
No action required.

Additional Information
If you have any questions regarding this Security Advisory, please contact your MultiTech sales representative or visit the technical resources listed below:

World Headquarters – USA
+1 (763) 785-3500 | sales@multitech.com

EMEA Headquarters – UK
+(44) 118 959 7774 | sales@multitech.co.uk

MultiTech Security Advisories
www.multitech.com/landing-pages/security
MultiTech monitors industry news and announcements to identity security issues that may impact our devices and operating systems and strive to provide the information and tools to keep your deployments secure and online.

MultiTech Developer Resources
www.multitech.net
An open environment where you can ask development related questions and hear back from MultiTech engineering or a member of this community.

Knowledge Base
http://www.multitech.com/kb.go
Immediate access to support information and resolutions for all MultiTech products.

MultiTech Support Portal
support.multitech.com
Create an account and submit a support case directly to our technical support team.

MultiTech Website
www.multitech.com

Trademarks and Registered Trademarks
MultiTech and the MultiTech logo are registered trademarks of Multi-Tech Systems, Inc. All other trademarks or registered trademarks are the property of their respective owners.

Revision History

Version	Author	Date	Change Description
-001	TG	12/14/2021	Published version
-002	DT	04/18/2023	Updated to include Vulnerability Note VU#930724, CVE-2021--4104, and CVE-2021-45046