MathWorks®
Accelerating the pace of engineering and science

MathWorks Response to CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 Apache Log4j vulnerabilities

Security researchers disclosed the following vulnerabilities in the Apache Log4j Java logging library:

- CVE-2021-44228: Apache Log4j2 JNDI features do not protect against attacker-controlled LDAP and other JNDI related endpoints
- CVE-2021-45046: The fix for CVE-2021-44228 was incomplete in certain non-default configurations.
- CVE-2021-45105: Apache Log4j2 Context Lookup features do not protect against uncontrolled recursion from self-referential lookups in certain non-default configurations
- CVE-2021-44832: Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server.

MathWorks Product Security promptly conducted an assessment across the code base for desktop, server and online applications and determined that MathWorks customers do not need to take any action related to MathWorks products and online applications.

MathWorks Desktop and Server Products

None of MathWorks general release desktop or server products include the affected versions of Log4j and so do not contain the CVE-2021-44228, CVE-2021-45046, or CVE-2021-45105. No version of released MATLAB implements the JDBC Appender by default. As such, MathWorks general release and server products are not vulnerable to CVE-2021-44832.

MathWorks is not aware of any exploitable vulnerabilities in the log4j framework used in any of our general release desktop or server products.

MathWorks general release desktop or server products include MATLAB, Simulink, Stateflow, MATLAB Production Server, MATLAB Web App Server, MATLAB Parallel Server, MATLAB Online Server, MATLAB Runtime, MathWorks Product Installer, MATLAB Runtime Installer, all Polyspace products, RoadRunner and any toolboxes or blocksets for any of these. In addition, this includes all previous general releases such as R2021b, R2021a, R2020b, R2020a, and so on.

MathWorks Online Applications

All online applications have been patched with officially suggested mitigations or confirmed as not vulnerable. After investigation there was no evidence that the vulnerability had been exploited on any of our systems.

Continuing Activities

The MathWorks, Inc.
3 Apple Hill Drive
Natick, MA 01760-2098
USA

Tel: 508.647.7000
Fax: 508.647.7001
info@mathworks.com
www.mathworks.com

MathWorks Product Security will continue to monitor this specific set of issues for their potential impact on our products.

Version 5: 30 March 2022

The MathWorks, Inc.
3 Apple Hill Drive
Natick, MA 01760-2098
USA

Tel: 508.647.7000
Fax: 508.647.7001
info@mathworks.com
www.mathworks.com