waratek

Customer Alert 20211220

Information on CVE-2021-45046: Remote Code Execution from JNDI Requests

What is CVE-2021-45046 about?
CVE-2021-45046 has been upgraded from a “LOW” CVSS Score of 3.7 to a “CRITICAL” 9.0 and explains how Log4j version 2.15.0 allows attackers to leak information using JNDI Lookup pattern and execute remote code in some environments. As of time when this advisory was posted, Log4j 2.16.0 and 2.12.2 fix this issue by removing support for message lookup patterns and disabling JNDI functionality by default. Only with Waratek can you keep your dependencies the same and secure your applications without any code changes, preventing errors from occurring due to the removal of the offending class.

Based on what we know now, can Waratek Java products mitigate this vulnerability?
Yes. Only Waratek provides a fully programmable security platform, ARMR, that can remediate vulnerabilities, including CVE-2021-45046. Unlike other security products that just attempt to block known exploit payloads, Waratek actually remediates the vulnerable code inside an application’s live executing code in real-time and with no interruption to service or degradation of performance.

Waratek is providing all customers an ARMR Remediation Patch which permanently remediates this vulnerability for live, executing Log4j code inside any workload or dependency.

Waratek recommends all customers to add the ARMR Remediation Patch for CVE-2021-45046 to their default ARMR security policy for all applications to permanently remediate the vulnerable code that enables this vulnerability. Modern Java applications that aren’t directly reliant on vulnerable versions of Log4j, but that have dependencies that are, will still benefit from the ARMR Remediation Patch.

As with all ARMR Rules and Remediation Patches, this permanent remediation can be applied live to any workload and does not require service restart or downtime to achieve permanent remediation.

Current Waratek customers can download the instant ARMR Remediation Patch via the Download Portal to permanently remediate this vulnerability for all workloads and applications. For assistance in deploying the patch, please contact our Customer Support team at support@waratek.com.

Does the vulnerability impact any third party tools I use with Waratek solutions?
According to Google, "More than 35,000 Java packages, amounting to over 8% of the Maven

Central repository (the most significant Java package repository), have been impacted by the recently disclosed log4j vulnerabilities."

We strongly recommend that all customers check third party support and advisory sites. If you have any questions or concerns, you can also contact our Customer Support team at support@waratek.com.

Non-Waratek customers should request a trial license or a live demonstration of Waratek's protective agents.

About Waratek
Some of the world's leading companies use Waratek's ARMR Security Platform to patch, secure and upgrade their mission critical applications. A pioneer in the next generation of application security solutions, Waratek makes it easy for security teams to instantly detect and remediate known vulnerabilities with no downtime, protect their applications from known and Zero Day attacks, and virtually upgrade out-of-support Java applications – all without time consuming and expensive source code changes or unacceptable performance overhead.

Waratek is the winner of the 2020 Cyber Defense Magazine's Cutting Edge Award for Application Security, the Cybersecurity Breakthrough Awards 2019 Overall Web Security Solution of the Year, and is a previous winner of the RSA Innovation Sandbox Award along with more than a dozen other awards and recognitions.