waratek

Customer Alert 20211210

Information on CVE-2021-44228: Remote Code Injection in Log4j

What is CVE-2021-44228 about?
Posted in the GitHub Advisory Database, CVE-2021-44228 explains how Log4j versions prior to 2.15.0 are subject to a remote code execution vulnerability via the ldap JNDI parser. *As of time when this advisory was posted, GitHub is still processing the vulnerability and advises to check back later for any additional information.*

Based on what we know now, can Waratek Java products mitigate this vulnerability?
Only Waratek provides a fully programmable security platform, ARMR, that can remediate vulnerabilities, including CVE-2021-44228. Unlike other platforms that just block vulnerabilities, Waratek actually remediates vulnerabilities inside an application's live executing code in real-time and with no interruption to service.

Customers who have applied ARMR's Socket:Connect rules to restrict connections to external locations have immediate mitigation for this vulnerability. Additionally, Waratek is providing all customers an ARMR Virtual Remediation Patch which permanently remediates this vulnerability for live, executing Log4j code inside any workload or software version.

Waratek recommends all customers to add the ARMR Virtual Remediation Patch for CVE-2021-44228 to their default ARMR security policy for all applications to permanently remediate the vulnerable code that enables this vulnerability. As with all ARMR Rules and Virtual Patches, this permanent remediation can be applied live to any workload and does not require service restart or downtime to achieve permanent remediation.

Waratek Customer Success Managers are contacting all customers to assist in applying the instant ARMR Remediation Patch to permanently remediate this vulnerability for all workloads and applications. For assistance in deploying the patch, please contact Customer Success at customersuccess@waratek.com.

Does the vulnerability impact any third-party tools I use with Waratek solutions?
We strongly recommend that all customers check third party support and advisory sites such as Elasticsearch and others, as the GitHub Advisory is still processing. 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 Award's 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.