waratek

Customer Alert 20211215

Information on CVE-2021-4104: Remote Code Execution from JNDI Requests

What is CVE-2021-4104 about?
CVE-2021-4104 explains how Log4j version 1.2 is vulnerable to deserialization of untrusted data when the attacker causes JMSAppender to perform JNDI requests that result in remote code execution. As of time when this advisory was posted, Apache is still processing this vulnerability and recommends ensuring no JMSAppender is configured for now.

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-2021-4104. Unlike other security products that just 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.

Waratek is providing all customers an ARMR 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 Remediation Patch for CVE-2021-4104 to their default ARMR security policy for all applications to permanently remediate the vulnerable code that enables their 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.

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 this vulnerability impact any third party tools I use with Waratek solutions?
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.