Mitigating the Apache Log4j Vulnerability

Overview

Log4Shell, the recently announced zero-day vulnerability affecting Apache Log4J, has been labeled by security experts as “the single biggest, most critical vulnerability of the last decade.” Experts are highly concerned due to the widespread usage of Log4j, how trivial it is to exploit, and the level of access given to attackers. For example, attackers can leverage a single line of code to gain full access to impacted systems and deploy ransomware. Recent security research shows that a single click of a malicious link from an employee can also trigger this vulnerability.

Remediation

The Cybersecurity & Infrastructure Security Agency has put out Emergency Directive 22-02 with recommended mitigation measures. Effective remediation requires identifying and patching all affected assets (all internally developed applications and software/hardware vendors utilized - see list of affected vendors below). In addition to patching, it is important to look for signs of compromise and exploitation as one of your systems may already be compromised.

Paladin Cyber, our risk engineering partner, has experts and tools to help with remediation available at no cost to you.

- Automated exploitability assessments
- Scanning tools to help identify affected assets
- Experts to support your remediation efforts
- Paladin Shield includes a browser extension that protects against WebSocket based Log4J exploits

To take advantage of these resources, please head to https://bcs.meetpaladin.com/ and sign up using your policy number. Email contact@meetpaladin.com with any questions.

Additional Resources

- Apache: Security Advisory
- CISA: Apache Log4j Vulnerability Guidance
- Blumira: An Analysis of The Log4Shell Alternative Local Trigger
- CISA: Technical Approaches to Uncovering and Remediating Malicious Activity
- CISA: Cybersecurity Incident & Vulnerability Response Playbooks
- CISA: Log4j (CVE-2021-44228) Affected Vendor & Software List