Apache Log4j Vulnerability: Supporting Clients

On Dec 9, 2021, exploit details were published regarding a high-risk vulnerability affecting Apache Log4j, a tool millions of applications use for logging purposes. Attackers can leverage this vulnerability, also known as Log4Shell, to gain full control of affected internet-facing systems using a single line of code, allowing for easier ransomware and malware deployment. No authentication is required for an attacker to compromise a system using this attack method.

On Dec 16, 2021, security researchers identified a new attack method that utilizes a web browser's Javscript WebSocket. Just navigating to a website by clicking a malicious link can trigger the vulnerability on systems that are not even exposed to a network. This development is especially concerning as it expands the attack surface beyond internet-facing systems.

Security researchers have already observed efforts to exploit this vulnerability from prominent ransomware gangs. All clients are advised to upgrade all impacted systems to version 2.17.0.

Relevant Security Vulnerabilities**:** CVE-2021-44228, CVE-2021-45046, CVE-2021-45105

How can you help your clients?

- Ensure clients are aware of the severity and widespread nature of the Log4j vulnerability

  Key Resources
  Apache: Security Advisory
  CISA: Apache Log4j Vulnerability Guidance
  CISA: ED 22-02: Apache Log4j Recommended Mitigation Measures

- Advise clients to identify and update all affected assets, including all internally developed applications and outside software/hardware products/vendors.

  Key Resources
  CISA: Log4j (CVE-2021-44228) Affected Vendor & Software List

- Recommend clients look for signs of compromise and exploitation

  Key Resources
  CISA: Technical Approaches to Uncovering and Remediating Malicious Activity
  CISA: Cybersecurity Incident & Vulnerability Response Playbooks

- Notify clients of risk management resources available through their insurer

  Example
  BCS cyber policyholders receive complimentary access to automated exploitability assessments, scanning tools to help identify affected assets, a browser extension to stop the WebSocket-based exploit, and remediation support through their Paladin Shield subscription.

Learn more about Paladin Cyber by visiting https://www.meetpaladin.com/ or reaching out to contact@meetpaladin.com.