Risk Services Bulletin – December 2021

Apache Log4j Vulnerability

Summary

HUB Risk Services Division is providing this risk advisory in response to an active and widespread exploitation of a vulnerability found in Apache's Log4j Java software library also referred to as "Log4Shell" and "Logjam." Due to its widespread use in Java desktop apps and its ease of exploit for hijacking systems remotely, this vulnerability is being described as one of the most severe in recent history. Industry experts have confirmed attacks exploiting this vulnerability starting as early as December 1, 2021.

Guidance

The NIST National Vulnerability Database has published a full description of CVE-2021-44228 here.

While information and guidance is rapidly evolving, the US Cybersecurity and Infrastructure Security Agency (CISA) has created, is regularly updating a webpage, *Apache Log4j Vulnerability Guidance*, and is actively maintaining a community-sourced GitHub repository of publicly available information and vendor-supplied advisories regarding the Log4j vulnerability. CISA is urging organizations to review their webpage and upgrade to Log4j version 2.15.0, or apply the appropriate vendor recommended mitigations immediately.

The Canadian Centre for Cyber Security posted alert AL21-019 in response to the Log4j vulnerability, which includes detection and mitigation guidance.

Industry experts indicate that the first signs of Log4Shell exploitation may have come weeks before the flaw was made public, suggesting that security teams should broaden their incident response investigations into possible compromise of their networks to December 1, 2021.

The Apache Log4j product team has also issued an official release containing detailed product information and mitigation recommendations.

Protecting People, Property, and Profitability

IT infrastructure and sensitive company or personal information can be compromised in many ways. Vendor breaches, compromised computer networks, and phishing scams are prevalent and the cyber threat landscape is evolving rapidly. This is a good time to reassess your organization's cybersecurity hygiene.

One source of resilience in the face of compounding crisis events and always-changing cyber risks is a comprehensive approach. If your organization doesn't have a current and active cyber, fraud, or continuity risk management program in place, the HUB Risk Services team can help.