SOLACE CYBER

APACHE LOG4J2

WHAT ACTION SHOULD YOU TAKE?

DECEMBER 2021

What is the Log4j vulnerability

And what action should be taken?

Executive Summary

Reports emerged on 9 December 2021 of a cyber security vulnerability, specifically a zero-day exploit, that is of significant concern to all organisations, posing one of the greatest security risks to the internet in recent times. The advanced ransomware lies within Log4j2 that is an open-source Java logging library developed by the Apache foundation. Java is a programming language, used routinely in many applications and is present in many services such as Microsoft's Minecraft, Apple iCloud, Twitter and Steam. Other affected platforms can include enterprise applications, cloud services and custom applications developed within an organisation.

Logging forms a crucial part of the run-time of these applications, providing a tool to understand a programs run-time behaviour and make it available for analysis. Because the usage of the logging framework is so highly adopted, data from businesses around the world that use these services could potentially become accessed by cyber criminals. Therefore, Solace Cyber recommend all organisations should take immediate action to mitigate the risk.

How Apache Log4j2 Exploit Works

The vulnerability within the Apache Log4j2 library enables unauthenticated remote code execution, which gives malicious attackers the ability to relentlessly scan and exploit digital systems automatically. Multiple attacks have already been deployed as part of this exploitation, using methods such as remote access backdoors known as Cobalt Strike Beacons, which is often a precursor to ransomware attacks.

What makes the Apache vulnerability particularly concerning, is that even after patching has taken place, your digital systems may have already been compromised.

A Critical Time

The Apache exploit comes at a crucial time for businesses. With many organisations experiencing the busiest time of the year, it is unlikely to be a coincidence that the exploit has surfaced so close to the holidays. Organisations should take action even if no signs of compromise are suspected yet, as it is expected that the risks to evolve throughout the Christmas and New Year period, particularly while many workplaces operate on minimal staffing.

Solace Cyber provide specialist cyber security services to organisations and can mitigate the risk of your company becoming exploited by the Log4j2 vulnerability.

Recommended Action to Mitigate the Risk of Apache Log4j2

Action 1: Identify

We recommend scanning all externally facing IPs to determine any systems that are at risk from this vulnerability or not patched. This should be the first priority for all businesses. Many enterprise applications have been working around the clock to create patching updates to restore security to potentially compromised systems.

Solace Cyber provide this as a service and can identify any compromised applications, using Nessus Professional with specially inserted plugins specifically to identify Log4J2.

Full identification with remediation guidance and advice will be given based on our findings.

Cost for Action 1: £350 +vat

Action 2: Detect and Respond

In addition to a vulnerability assessment, Solace Cyber recommend the installation of Endpoint Detection and Response (EDR) agents onto each device that is identified as at risk. EDR is the next generation of cyber security solutions, utilising machine learning to continually evolve in ways that traditional anti-virus is unable to. This provides critical protection against Log4j2, which will monitor and proactively protect against payloads delivered by an actively exploited system.

Solace Cyber technical team use FortiEDR software, with additional threat hunting and scanning tools, which are used to scan for evidence of exploitation and other known risks against all servers which are at risk.

This service is available with Solace Cyber and includes monitoring by our 24/7 Security Operations Centre (SOC) until the new year, to provide peace of mind throughout the holiday season when Log4j1 attacks are likely to become heightened.

Cost for Action 1 & 2: £995 +vat

Request a call back from Solace Cyber to enquire or initiate actions listed above here

Technical Details – Apache Log4j2 Vulnerability (CVE-2021-44228)

The vulnerability, tracked as CVE-2021-44228 and referred to as "Log4Shell," affects Java-based applications that use Log4j 2 versions 2.0 through 2.14.1. Log4j 2 is a Java-based logging library that is widely used in business system development, included in various open-source libraries, and directly embedded in major software applications. The scope of impact has expanded to thousands of products and devices.

Because this vulnerability is in a Java library, the cross-platform nature of Java means the vulnerability is exploitable on many platforms, including both Windows and Linux. As many Java-based applications can leverage Log4j 2, organisations should contact application vendors or ensure their Java applications are running the latest up-to-date version. Developers using Log4j 2 should ensure that they are incorporating the latest version of Log4j into their applications as soon as possible in order to protect users and organisations.

For further details, please email cyber@solaceglobal.com or give us a call on +44 (0) 1202 308 810.