AL2021_58 Apache Issues 3rd Patch to Fix New High-Severity Log4j Vulnerability (23rd December 2021)

Description

The Apache Software Foundation (ASF) released another patch for Log4j on Friday, version 2.17.0, which might be abused by hostile actors to stage a denial-of-service (DoS) attack.

Summary

The new vulnerability, designated CVE-2021-45105 (CVSS score: 7.5), affects all versions of the tool from 2.0-beta9 to 2.16.0, which the open-source charity group released earlier this week to remedy a second flaw that could contribute to remote code execution (CVE-2021-45046). This was caused due to an "incomplete" fix for CVE-2021-44228, also recognized as the Log4Shell flaw.

How it works

In an updated alert, the Apache Software Foundation revealed that "Apache Log4j2 versions 2.0-alpha1 through 2.16.0 did not defend against uncontrolled recurrence from self-referential lookups." "When the logging configuration uses a non-default Pattern Layout with a Context Lookup (for example, $$ctx:loginId), attackers with control over Thread Context Map (MDC) input data can craft malicious input data that contains a recursive lookup, resulting in a StackOverflowError that kills the process."

The bug was discovered by Akamai Technologies' Hideki Okamoto and an anonymous vulnerability researcher. CVE-2021-45105 does not affect Log4j versions 1.x, though.

It's should be noted that CVE-2021-severity 45046's score has been revised from 3.7 to 9.0 to reflect the fact that an attacker could exploit the flaw to send a specially crafted string that results in "information leak and remote code execution in some environments and local code execution in all environments," confirmed in a previous report by Praetorian security researchers.

It was also stated by the project maintainers that Log4j versions 1.x are no longer supported and that security problems discovered after August 2015 will not be patched to urge users to switch to Log4j 2 to receive the most recent fixes.

The US Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive that requires federal civilian departments and agencies to patch their internet-facing systems for the Apache Log4j vulnerabilities by December 23, 2021, citing the flaws as an "unacceptable risk."

Log4j weaknesses have become a profitable attack vector and a focus point for many threat actors, including nation-backed hackers from China, Iran, North Korea, and Turkey as well as the Conti ransomware group, to carry out a variety of follow-on malicious actions. This is the first time a sophisticated crimeware cartel has been aware of the vulnerability.

"The present exploitation resulted in several use cases through which the Conti group investigated the potential of employing the Log4j 2 vulnerability," according to AdvIntel researchers. "The criminals pursued targeting specific vulnerable Log4j 2 VMware vCenter [servers] for lateral movement directly from the compromised network, resulting in vCenter access affecting victim networks in the United States and Europe from the pre-existing Cobalt Strike sessions," says the report.

Cryptocurrency miners, botnets, remote access trojans, initial access brokers, and a new ransomware strain known as Khonsari are among those who have taken advantage of the vulnerability. Check Point, an Israeli security firm, said it had logged over 3.7 million exploitation attempts so far, with recognized criminal groups responsible for 46% of those attacks.

Remediation

At this moment there is no fixed patch to remedy this new vulnerability. However, researchers from ASF advise users to implement the following security measures below.

- Update log4j to the latest update - Software updates are vital because they frequently include critical security patches. Software updates might contain new or enhanced features, as well as improved compatibility with different devices or applications, in addition to security fixes.

- Desist from using log4j version 1x – this version is no longer supported by apache. Therefore, any vulnerability found, will not be patched.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Apache issues 3rd patch to fix new high-severity Log4j vulnerability (18th December 2021). Retrieved from thehackernews.

  https://thehackernews.com/2021/12/apache-issues-3rd-patch-to-fix-new-high.html

- Apache issues 3rd patch to fix new high-severity Log4j vulnerability (15th December 2021). Retrieved from thehackernews.

  https://thehackernews.com/2021/12/hackers-begin-exploiting-second-log4j.html

- Apache issues 3rd patch to fix new high-severity Log4j vulnerability (20th December 2021). Retrieved from Center for Internet Security.

  https://www.cisecurity.org/log4j-zero-day-vulnerability-response/