AL2021_56 Second Log4j Vulnerability (CVE-2021-45046) Discovered (21st December 2021)

Description

The Apache Software Foundation (ASF) has released a new patch for the Log4j logging application after the previous fix for the recently disclosed that the Log4Shell exploit was deemed "incomplete in certain non-default settings."

Summary

Its initial vulnerability, CVE-2021-45046, is rated 9/10 on the CVSS scoring system and impacts all versions of Log4j from 2.0-beta9 to 2.12.1 and 2.13.0 to 2.15.0, which the project maintainers released last week to address a critical remote code execution vulnerability (CVE-2021-44228) that could be exploited to penetrate and seize command of system applications.

How it works

The unfinished patch for CVE-2021-44228, according to ASF researchers, could be used to "create malicious input data using a Java Naming Directory Interface (JNDI) lookup pattern, eventually resulting in a denial-of-service (DoS) attack." The most recent version of Log4j, 2.16.0 (for clients requiring Java 8 or later), disables JNDI by default and practically kills support for message lookups. Users that still need Java 7 should upgrade to Log4j version 2.12.2 as soon as it is released.

The ASF's Ralph Goers stated, "Dealing with CVE-2021-44228 has proven that the JNDI has serious security flaws.Though we have mitigated what we are aware of, it would also be safer for users if it were turned off by default, especially because the vast majority are unlikely to utilize it."

JNDI (Java Naming and Directory Interface) is a Java API that lets Java programs search for data and resources like LDAP servers. Log4Shell is a component of the Log4j library, an open-source Java-based logging system commonly used in Apache web servers.

The problem arises whenever the LDAP connector's JNDI component is used to inject an malicious LDAP request — something like "$jndi:ldap:/attacker controlled website/payload to be executed" — that, when logged on a web server

running the vulnerable version of the library, allows an adversary to retrieve a payload from a remote domain and execute it locally.

The current patch comes as a "real cyber pandemic" that has erupted as a result of the weakness, with various threat actors exploiting Log4Shell in ways that set the framework for future assaults, such as running coin miners, remote access trojans, and ransomware on vulnerable machines. The opportunistic intrusions are alleged to have started at least on December 1st 2021, even though the flaw was first discovered on December 9th, 2021.

Because the security hole exists in an almost universally used logging framework in Java apps, malicious actors now have an unprecedented gateway to enter and corrupt millions of devices across the globe.

The remotely exploitable flaw also affects hundreds of major enterprise products from several companies, including

- Akamai
- Amazon
- Apache
- Apereo
- Atlassian
- Broadcom
- Cisco
- Cloudera
- ConnectWise
- Debian
- Docker
- Fortinet
- Google
- IBM
- Intel
- Juniper Networks
- Microsoft
- Okta
- Oracle
- Red Hat

SolarWinds

- SonicWall • Splunk
- Ubuntu
- VMware • Zscaler

- Zoho

"Unlike all the other big hacks that only use one or a few pieces of software, Log4j is almost ubiquitous in Java-based products and online services. It's extremely difficult to fix it manually”-Check Point, an Israeli security firm stated. "Because of the difficulty in patching it and the ease with which it can be exploited, it appears that this vulnerability will be with us for years to come unless organizations and services take prompt action to prevent assaults on their products by providing a safeguard."

Ten different parties have joined on the exploit bandwagon in the days since the issue was discovered, and around 44% of business networks around the world have already been compromised, indicating a considerable escalation. Furthermore, criminal gangs posing as access brokers have started exploiting the vulnerability to get initial access to target networks, which can see them selling access to other associates.

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.
- Disable JNDI settings - The Java Name and Directory InterfaceTM (JNDI) is a programming interface (API) for applications built in the JavaTM programming language that provides naming and directory capabilities. It is designed to work with any directory service solution.

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

References

- The second Log4j vulnerability (CVE-2021-45046) was discovered (14th December 2021). Retrieved from thehackernews.

  https://thehackernews.com/2021/12/second-log4j-vulnerability-cve-2021.html

- The second Log4j vulnerability (CVE-2021-45046) was discovered (15th December 2021). Retrieved from Check Point.

  https://blog.checkpoint.com/2021/12/13/the-numbers-behind-a-cyber-pandemic-detailed-dive/

- The second Log4j vulnerability (CVE-2021-45046) was discovered (13th December 2021). Retrieved from Apache.

  https://logging.apache.org/log4j/2.x/security.html