Log4j Vulnerability Affects Multiple Apache and Legacy Services; Exploit Code Publicly Released

Vulnerability Bulletins	◯ TLP:WHITE	Alert ID : ea51506b	Dec 10, 2021, 01:27 PM

Proof-of-concept exploit code for a critical zero-day vulnerability, designated CVE-2021-44228, in the Apache Log4j Java-based logging library has been released publicly, exposing enterprises and services to remote code execution (RCE) attacks by attackers.

The Health-ISAC Threat Operations Center has released a brief survey regarding your observed experiences with this vulnerability, please utilize the link here. Your assistance is greatly appreciated. This alert has additional technical details and recommendations, which can be accessed below.

Additional Info

Log4j, and its successor Log4j2, are developed by the Apache Foundation and are widely used by both enterprise apps and cloud services for logging purposes. Systems and services that use Log4j between versions 2.0-beta9 and 2.14.1 are all affected by CVE-2021-44228, which includes many services and applications written in Java. The vulnerability allows for repeated and reliable unauthenticated remote code execution in targeted environments.

The vulnerability was first discovered in the popular Java-based game Minecraft but researchers warn that other cloud applications are also vulnerable. Log4j is incorporated into a host of popular frameworks, including Apache Struts2, Apache Solr, Apache Druid, and Apache Flink. That means that a large number of third-party apps may also be vulnerable to exploits that carry the same high severity as those threatening Minecraft users.

In analyzing CVE-2021-44228, security firm Randori determined the following:
- Default installations of widely-used enterprise software are vulnerable to CVE-2021-44228.
- CVE-2021-44228 can be exploited reliably and without authentication.
- CVE-2021-44228 affects multiple versions of Log4j 2.
    - The United States Cybersecurity and Infrastructure Security Agency (CISA) Cyber Information Sharing and Collaboration Program (CISCP) has stated that CVE-2021-44228 affects Log4j versions 2.0-beta9 to 2.14.1.
- CVE-2021-44228 allows for remote code execution as the user running the application that utilizes the library.

There already are several reports of malicious servers performing Internet-wide scans in attempts to locate vulnerable servers. Due to the ease of exploitation and the breadth of applicability, we suspect ransomware actors to begin leveraging this vulnerability immediately, said the Randori security team.

Available Patch

Available

CVE(s)

CVE-2021-44228

Recommendations

- Administrators should identify apps and services that rely on Log4j or Log4j2 for critical processes
- Apache has released Log4j 2.15.0 to address CVE-2021-44228. Those using the Log4j library are advised to upgrade to the latest release as soon as possible seeing that attackers are already searching for exploitable targets.
  - The exploit can also be mitigated in previous releases, 2.10 and later, by setting system property log4j2.formatMsgNoLookups to "true" or removing the JndiLookup class from the classpath.
- Block any outgoing traffic that is not required by your organization's requirements.
  - If your organization has a server running a Java application that only needs to accept incoming traffic, prevent all outgoing traffic.
- If you believe you may be impacted by CVE-2021-44228, Health-ISAC encourages all organizations to adopt an assumed breach mentality and review logs for impacted applications for unusual activity.
  - If anomalies are found, we encourage you to assume that you may have been compromised and treat this as an active incident and respond accordingly.

Release Date

Dec 10, 2021

Sources

Ars Technica: Zero Day in Ubiquitous Log4j Tool Poses a Grave Threat to the Internet
ZDNet: Security Warning: New Zero-day in the Log4j Java Library Is Already Being Exploited
BleepingComputer: New Zero-day Exploit for Log4j Java Library Is an Enterprise Nightmare
Apache: Download Apache Log4j 2
Randori: CVE-2021-44228 – Log4j 2 Vulnerability Analysis
CISA: Apache Releases Log4j Version 2.15.0 to Address Critical RCE Vulnerability Under Exploitation

Reference | References

Ars Technica

Twitter
randori
Apache
ZDNet
cisa

Tags

CVE-2021-4422, Log4j, Apache Web server, Apache Struts2, Apache

---

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Intel 471 - Vulnerability Advisories: Intel 471's Common Vulnerabilities and Exposures (CVE) Vulnerability Advisories are a quick reference tool designed to assist in patch prioritization and vulnerability management decision-making. These advisories track the life cycle of significant vulnerabilities from initial disclosure to exploit weaponization and productization observed in the underground.