VULNERABILITY BULLETINS

Update: CISA Releases Central Guide and Affected Product Repository for Log4j Vulnerability

TLP:WHITE

Dec 20, 2021

**** Update****

The Health-ISAC Threat Operations Center (TOC) continues to track ongoing developments regarding the weaponization and mitigation of CVE-2021-44228 in the logging library known as Log4j.

The United States Cybersecurity and Infrastructure Security Agency (CISA) has released a central repository of technical alerts, mitigation guides, and other relevant pieces of information related to CVE-2021-44228, which can be accessed here. CISA has also released an accumulated table of affected products and service providers, which can also be accessed here. The information in the repository is provided "as is" for informational purposes only and is being assembled and updated by CISA through collaboration with the broader cybersecurity community.

Akamai has also released their key findings on CVE-2021-44228, examining targeting strategies and exploit mutations from motivated threat actors, which can be accessed here.

Health-ISAC's TOC will continue to monitor developments as they become available. The TOC will continue to aggregate relevant Indicators of Compromise (IOCs) and ingest them into our automated threat-sharing platform, Health-ISAC Indicator Threat Sharing (HITS). If you have IOCs you think would be valuable to the Health-ISAC member community, feel free to share them with the TOC, by emailing toc@h-isac.org.

**** End of 12/30/2021 Update, 12/30/2021 Update Below ****

The Health-ISAC Threat Operations Center (TOC) has been closely tracking ongoing developments regarding the weaponization and mitigation of CVE-2021-44228 in the logging library known as Log4j. As a result of the critical vulnerability, the Health-ISAC Threat Intelligence Committee (TIC) has subsequently raised the Cyber Threat Level to Yellow (ELEVATED). The TOC has also provided new information and materials for organizations to increase their security posture in their internal technological environment.

Observed instances of malicious actors scanning for CVE-2021-44228-vulnerable servers have been recorded by numerous public and private entities, as cybersecurity researchers at Sophos have warned that they've detected hundreds of thousands of attempts to remotely execute code using the Log4j vulnerability, along with extensive scans looking for CVE-2021-44228-vulnerable servers. Cybersecurity researchers at Check Point are warning that they are also detecting over 100 attempts to exploit CVE-2021-44228 every minute. Additionally, researchers have observed actors utilizing CVE-2021-44228 to install cryptocurrency-mining malware on systems and improve botnet installation capabilities.

In order to prevent successful exploitation of CVE-2021-44228, the National Computing Centre (NCC) Group has posted several network-detection rules to detect exploitation attempts and indicators of successful exploitation. Microsoft has also released its set of indicators of compromise and subsequent guidance for preventing attacks on Log4j vulnerability.

The TOC has also generated an informational presentation on CVE-2021-44228, which includes an executive summary, technical details, and recommendations. This slide deck is available for all members to disseminate and present within their organization, the deck is attached to this alert, and can also be accessed here.

**** End of 12/30/2021 Update, Original Update Below ****

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.

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.

Reference(s)	Ars Technica, Twitter, randori, Apache, ZDNet, cisa, cisa, GitHub

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 20, 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

Alert ID b8e75bce

This Alert has 2 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

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.

Download Health-ISAC’s Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.