DECEMBER 14, 2021

LOG4J 2/LOG4SHELL (CVE-2021-44228)

Log4j is an open-source logging framework/library which allows software developers to log various data within their application. This data can include user input and is used ubiquitously in Java applications, especially enterprise software.

Analyst Note: Log4j 2 is the logging framework. Log4Shell is the vulnerability (CVE-2021-44228).

Log4Shell Description

Apache Log4j 2 version 2.0-beta9 to 2.14.1 contains a vulnerability in the method JNDI uses to resolve variables. JNDI fails to sanitize parameters such as URLs, User Agent strings, host names, and any other client controllable string that can be written to disk as a log. An attacker can craft a request sent to a vulnerable server to execute arbitrary code loaded from attacker-controlled infrastructure when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. Updating to 2.16.0 is advised to resolve a DoS vulnerability. If an update to the current version is not viable, a workaround for previous releases (>2.10) can be implemented by setting system property "log4j2.formatMsgNoLookups" to “true” or it can be mitigated in prior releases (<2.10) by removing the JndiLookup class from the classpath (example: zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class). (Sources: NVD, MSFT)

Significant Findings

- Fixes for Log4j in 2.15.0 version incomplete (Apache)
- Report of Log4j being leveraged to distribute ransomware (Bitdefender)
    - Ransomware sample (VirusTotal)
- Additional CVE identified: CVE-2021-4104 (NVD)
- Additional CVE identified: CVE-2021-45046 (NVD)
- Users seeing obfuscated exploit attempts (Link redacted.)
- RH-ISAC members seeing scanning attempts (Link redacted.)
- Ten families of malicious samples spreading using Log4j 2 vulnerability (Netlab 360)

RH-ISAC Actions Taken

- Hosted RH-ISAC Members-Only Weekly Intelligence Call with a Log4j focus
- Continued posting updates to Member Exchange Tracking Page
- Attended CISA call
- Attended Flashpoint Intelligence/Risk-Based Security webinar covering the Log4j vulnerability

- Vetted member-shared IOCs associated with Log4Shell, and as of 12:00PM ET, all current IOCs are now in the RH-ISAC TruSTAR vetted enclave and will be updated regularly
- Conducted analysis of SOHO routers to determine if they are vulnerable to the Log4Shell vulnerability
- Confirmed that RH-ISAC collaboration tools do not appear vulnerable to log4j vulnerability

Intelligence Collected and Reviewed

- CISA Log4j guidance (CISA)
- Sigma rule for detecting obfuscation against log4j RCE vulnerability (GitHub)
- Member-submitted Unicode bypass code (Link redacted.)
- Log4j 2.16.0 released (Apache)
- Python POC for Log4j vulnerability (GitHub)
- Member-created regex that detects 99%+ of the bypasses (Link redacted.)
- CISA community-sourced Log4j GitHub repo (GitHub)
- Open-source blog with recommendations on mitigation (Swiss Government CERT)
- Log4Shell IOCs (GitHub)
- List of applications affected by Log4j vulnerability (GitHub)
- Products affected by Log4j vulnerability, compiled by Dutch NCSC-NL (GitHub)
- Log4j Vulnerability Tester (TrendMicro)

Upcoming Events

- Webinar from Tenable for those users of Tenable products
  - Register at Tenable
- Webinar from Recorded Future
  - Register at Recorded Future