LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY

HC3: Sector Alert

December 17, 2021 TLP: White Report: 202112171300

Active Exploitation of Log4j (Update 1)

Executive Summary

This is Update 1 of a Sector Alert published on December 10. A highly-utilized application called Log4j contains several vulnerabilities, the most severe of which is being actively and aggressively attacked by foreign countries and cybercriminals alike. Upon successful exploitation, a compromised system or device can be used to execute arbitrary code, which can serve as the beginning of a larger cyberattack potentially resulting in further effects, including data exfiltration and ransomware. HC3 advises healthcare and public health organizations to survey their infrastructure and ensure they are not running vulnerable versions of Log4j. Any vulnerable systems should be upgraded and a full investigation of the enterprise network should commence to identify possible further exploitation of their information infrastructure.

Report

This is Update 1 of a Sector Alert published on December 10. Log4j is a very common Java library/framework that provides logging capabilities to any number of software platforms that it serves. In November, a remote code execution vulnerability (CVE-2021-44228) was identified in certain versions of Log4j which are now being actively exploited. Proof-of-concept exploit code has been circulating social media since December 9 and is publicly posted on well-known code repositories. There are additional vulnerabilities that have been since been discovered in Log4j which should be considered as well. Some of those are detailed in this article. HC3 highly recommends that healthcare entities maintain their situational awareness specifically with regard to Log4j vulnerabilities as it is likely that, with the increased scrutiny and visibility associated with the known vulnerabilities, additional vulnerabilities will be discovered and released to the public in the near future.

Analysis

Log4j is widely deployed throughout the health sector, as in other industries. It's a common application, utilized by many enterprise and cloud applications, including several large and well-known vendors. Therefore, it's highly likely that the health sector is impacted by this vulnerability, and possibly to a large-scale extent. Log4j is known to be a component in many software platforms, some of which are part of cloud services. The SANS Institute posted an analysis of exploitation, which contains already outdated patching information. HC3 recommends treating these vulnerabilities as a high-priority. A large and growing number of large vendors have been developing and releasing patches specific to these vulnerabilities. HC3 expects this list to continue to grow.

Vulnerabilities

The most egregious vulnerability (CVE-2021-44228) is a remote code execution vulnerability which was discovered in later November, however the release and circulation of proof-of-concept exploit code in recent days has made this an even higher priority. The Log4j software is maintained by Apache and they have released an update which should be deployed (after testing, as needed) across all vulnerable devices in the enterprise in a timely manner to address CVE-2021-44228. Apache discusses the vulnerability in further detail here. They have also made release notes available for this version. This vulnerability is also known as Log4Shell and it applies to versions 2.0-beta up to 2.14.1. At the time this alert is being published, an update to the most recent version of Log4j – version 2.16.0 – will mitigate all known vulnerabilities. Healthcare entities are advised to continue to monitor for updated versions of Log4j.

Patches, Mitigations, and Workarounds

One researcher shared Yara rules for detection of active exploitation. As Apache has noted, the vulnerability can 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. Most importantly, Apache has made the most recent version of the software available, version 2.16.0, and highly recommends upgrading to it. HC3 echoes this recommendation and implores the HPH to address infrastructure in a comprehensive and timely manner. Upgrading is the ideal solution but other mitigation actions listed above can be sufficient until a full upgrade becomes a viable choice. The Cybersecurity & Infrastructure Security Agency (CISA), part of the Department of Homeland Security, maintains a website dedicated to this vulnerability which is frequently updated. CISA also maintains a GitHub page. Furthermore, Apache maintains a page dedicated to Log4j security, and it will be critical for healthcare organizations to check back at this page frequently for updates. As of the publishing of this alert, Log4j version 2.16.0 is the most up-to-date version available. However, we anticipate further updates being released in the near future, which will be detailed and available on this site. There are freely-available scanning tools provided by various security vendors to identify vulnerable versions of Log4j. While HC3 does not endorse any of these tools specifically, healthcare organizations might find it valuable to identify a free or commercially available tool to assist them in identification of vulnerable systems and devices. As always, appropriate cautions should be taken when selecting and utilizing such tools.

References

New zero-day exploit for Log4j Java library is an enterprise nightmare
https://www.bleepingcomputer.com/news/security/new-zero-day-exploit-for-log4j-java-library-is-an-enterprise-nightmare/

Apache Log4j Security Vulnerabilities
https://logging.apache.org/log4j/2.x/security.html

Apache release notes for Log4j version 2.15.0
https://logging.apache.org/log4j/2.x/changes-report.html#a2.15.0

Apache: Limit the protocols jNDI can use and restrict LDAP.
https://issues.apache.org/jira/browse/LOG4J2-3201

NIST NVD: CVE-2021-44228
https://nvd.nist.gov/vuln/detail/CVE-2021-44228

Apache/logging-log4j2
https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc1

Remote code injection in Log4j
https://github.com/advisories/GHSA-jfh8-c2jp-5v3q

CISA Log4j Vulnerability Guidance website
https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

Zeroday in ubiquitous Log4j tool poses a grave threat to the Internet
https://arstechnica.com/information-technology/2021/12/minecraft-and-other-apps-face-serious-threat-from-new-code-execution-bug/

Download Apache Log4j 2
https://logging.apache.org/log4j/2.x/download.html

Log4j zero-day gets security fix just as scans for vulnerable systems ramp up
https://therecord.media/log4j-zero-day-gets-security-fix-just-as-scans-for-vulnerable-systems-ramp-up/

YfryTchsGD - Log4jAttackSurface
https://github.com/YfryTchsGD/Log4jAttackSurface

RCE in log4j, Log4Shell, or how things can get bad quickly
https://isc.sans.edu/forums/diary/RCE+in+log4j+Log4Shell+or+how+things+can+get+bad+quickly/28120/

GitHub: Proof of Concept exploit code
https://github.com/tangxiaofeng7/apache-log4j-poc

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback