U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00236

UPDATE ON LOG4SHELL VULNERABILITIES

DATE ISSUED: 23rd December 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

The Log4Shell vulnerabilities associated with the Log4j Java logging component have evolved and further patches have been released by Apache, requiring further updates to all affected software and servers. Details of subsequent vulnerabilities and patching can be found below.

BREAKDOWN

Subsequent vulnerabilities have been discovered in connection with the initial Log4j library zero-day (CVE-2021-44228) and patches have been released by Apache who are working diligently with security teams around the globe working to secure their systems. The new vulnerability is being tracked as CVE 2021-45046, as the original fixes were not complete for certain configurations. Version 2.16.0 has been released to cover this Denial of Service vulnerability, however this release does is still vulnerable to another DoS vulnerability CVE-2021-45105 and version 2.17.0 has now been released.

REMEDIATION STEPS

- Apply latest update released by Apache to upgrade to Log4j 2.17.0. This update requires Java 8 or greater. If you are running Java 7 and cannot upgrade, install Log4j 2.12.2 released by Apache (see GitHub & Google resources for a list of affected software, please note this list may not be 100% inclusive of all potentially vulnerable software)
- If you are unable to apply the patch and have version 2.10 and above CERT and Sophos have provided mitigation instructions. See resource below. This mitigation will not mitigate the new DoS vulnerability.
- Apply third-party patches as they become available
- Set up alerts on devices running Log4j to detect probes or attacks.
- Scan for known-bad versions of Log4j by file hash – unfortunately due to the manner in which Log4j is utilised and bundled into some services and software this will only detect some, not all.
- Implement a Web Application Firewall (WAF) in front of all Internet facing services

REFERENCES & RESOURCES

Apache	https://logging.apache.org/log4j/2.x/security.html
Threatpost	https://threatpost.com/java-supply-chain-log4j-bug/177211/
Google Security Blog	https://security.googleblog.com/2021/12/understanding-impact-of-apache-log4j.html
GitHub Repository	https://github.com/NCSC-NL/log4shell/blob/main/software/README.md
ZDNet	https://www.zdnet.com/article/second-log4j-vulnerability-found-apache-log4j-2-16-0-released/ https://www.zdnet.com/article/apache-releases-new-2-17-0-patch-for-log4j-to-solve-denial-of-service-vulnerability/
CERTNZ	https://www.cert.govt.nz/it-specialists/advisories/log4j-rce-0-day-actively-exploited/