UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00232

LOG4SHELL REMOTE CODE EXECUTION VULNERABILITY

DATE ISSUED: 14th December 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

A Java logging component in the widely used in an extensive range of software is vulnerable to a zero-day Remote Code Execution (RCE) attack, with the potential to affect millions, known as Log4Shell (CVE-2021-44228).

BREAKDOWN

This vulnerability gets its name from the popular Java logging library Apache Log4j v2.10 and 2.14.1, and the fact that an unauthenticated attacker can pretty much spin up their own Shell to run whatever code they like remotely. This is possible due to improper input validation when a vulnerable serve us sent a "loaded" piece of data that would be expect a server to write to its logfile, such as an HTTP header. The booby-trap is sprung while the server checks for a valid Java program and runs the file to assist with logging. By default, unpatched versions of Log4j allow logging requests to initiate LDAP searches and other online lookups – in other words data being logged can set off server-side code execution and may reach out to malicious servers. First publicly disclosed on the 9th December, researchers are now suggesting that it has been exploited as early as December 1st. Known cyber threat actors, groups, botnets and cryptominers are scanning the Internet to locate vulnerable instances. The Log4j library is utilised in numerous forms across thousands of enterprise and open source software, cloud platforms, web apps and email servers. It is highly likely that an organisation may be unaware that this Log4j is present in their environment and should work to determine whether vulnerable, Internet-facing devices are present and require patching.

REMEDIATION STEPS

- Apply latest update released by Apache to upgrade to Log4j 2.15.0 (see GitHub Resource 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.
- 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	http://mail-archives.apache.org/mod_mbox/www-announce/202112.mbox/%3CD88D40C5-8884-470E-8FA3-3B6D6899A7B0@apache.org%3E
GitHub Repository	https://github.com/NCSC-NL/log4shell/blob/main/software/README.md
ZDNet	https://www.zdnet.com/article/log4j-rce-activity-began-on-december-1-as-botnets-start-using-vulnerability/
CERT NZ	https://www.cert.govt.nz/it-specialists/advisories/log4j-rce-0-day-actively-exploited
Sophos	https://news.sophos.com/en-us/2021/12/12/log4shell-hell-anatomy-of-an-exploit-outbreak/