NETTITUDE
AN LRQA COMPANY

Threat Intelligence Briefing: Log4Shell

Intelligence Summary (17 Dec Update)

Date: 17 DECEMBER 2021
Version: 1.0

Contents

1 LATEST INFORMATION.....4

1 Latest Information

As of 17 December 2021, further reporting indicates that despite previous mitigations and patching, version 2.15.0 of Log4J remains vulnerable. The previous vulnerability (CVE-2021-45046) could allow for local denial of service (DoS) attacks. As such the impacts of the vulnerability were thought to be limited. With a huge number of cybersecurity researchers studying the patched Log4J 2.15.0 version it came to light this morning (17 December) that the same vulnerability (CVE-2021-45046) in Log4j version 2.15.0 is more serious than previously thought and allows for the exfiltration of sensitive data.

Now that the vulnerability offers the potential for data exfiltration, Apache have raised the base CVSS risk score from 3.7 (Low) to 9.0 (Critical). The risk associated with this vulnerability is increased more so by the publication of Proof of Concept (PoC) code. There is now PoC code on the indexed web that describes and demonstrates the vulnerabilities use. This will make the utilisation of the vulnerability much clearer to researchers and unfortunately threat actors.

Log4j version 2.15.0 remains a critical cybersecurity threat to organisations.

Nettitude cannot emphasise enough the need to update log4J version 2.15.0 to version 2.16.0 as soon as possible. In order for users to upgrade to Log4J version 2.16.0 Java 8 or later is required. Where upgrading is not possible, guidance remains to consult with product vendors to determine the overall risk. Defence in depth is vital. Other mitigations such as egress filtering to prevent the outbound callbacks that download the malicious binaries should be put in place.

LINKS:
Log4j 2.15.0 stills allows for exfiltration of sensitive data - Praetorian
https://www.praetorian.com/blog/log4j-2-15-0-stills-allows-for-exfiltration-of-sensitive-data/

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

NETTITUDE

AN LRQA COMPANY

UK Head Office
Jephson Court, Tancred Close, Leamington Spa, CV31 3RZ

Americas
50 Broad Street, Suite 403, New York, NY 10004

Asia Pacific
1 Fusionopolis Place, #09-01, Singapore, 138522

Europe
Leof. Siggrou 348 Kallithea, Athens, 176 74
+30 210 300 4935

Follow Us

solutions@nettitude.com
www.nettitude.com