TLP White

Advisory: 2021-007: Log4j vulnerability – advice and mitigations

On 10 December 2021, ACSC released an alert relating to a serious vulnerability in versions of the Log4j Java logging library. Malicious cyber actors are using this vulnerability to target and compromise systems globally and in Australia. The ACSC is working with a significant number of victims and affected vendors across all sectors of the economy.

The fifth edition of this Advisory is current as of 0930 AEDT, 29 December 2021 and has been updated to include the CVE-2021-44832 vulnerability.

What is Log4j?

Log4j is a key software building block found in a wide variety of Java applications. It provides logging functionality in many products ranging from messaging, productivity and video conference applications, to webservers and video games. Over 100,000 products from hundreds of vendors – and in house developed software – may contain Log4j.

What is the impact?

The Log4j vulnerability – otherwise known as CVE-2021-44228 or Log4Shell – is trivial to exploit, leading to system and network compromise. If left unfixed malicious cyber actors can gain control of vulnerable systems; steal personal data, passwords and files; and install backdoors for future access, cryptocurrency mining tools and ransomware.

Who is affected by this?

Individuals should **update all applications as soon as vendor patches become available.** Make sure your devices and applications are secure by updating regularly and setting automatic updates where possible.

Organisations should follow the prioritised mitigations in this Advisory: contact their vendors, implement suggested mitigations, and **update their applications as soon as vendor patches become available.** Organisations that have developed in house software should check for use of Log4j and upgrade to the latest version of Log4j, or consider disabling the `JndiLookup` class. Even applications which do not appear affected, or are not written in Java may need updating if Log4j is used in a backend system.

Vendors should follow the prioritised mitigations in this Advisory: identify their use of Log4j and update to the latest version, consider disabling the `JndiLookup` class, and work to develop the required patches or mitigation advice to assist customers remediate the vulnerability.

Vendors and organisations should continue to monitor their systems and networks for compromise or suspicious activity, even after remediation steps or patching has been completed, and remain alert to future advisories.

Vulnerability Details

The Log4j Java logging library is one of the most widely used Java-based logging utilities globally. Due to its widespread use in popular software and hardware platforms – such as messaging and productivity applications, mobile device managers, teleconference software, web hosting, and even video games – a large number of third-party applications

may also be vulnerable to exploitation. Google estimates that more than 35,000 Java packages may be affected, **80 times more than the median Java vulnerability.**

- CVE-2021-44228: Is a vulnerability in versions of Log4j prior to 2.15 which allows a malicious actor to download a payload through an encapsulated Java Naming and Directory Interface (JNDI) request, resulting in remote code execution (RCE). The Common Vulnerability Scoring System (CVSS) rates this vulnerability as Critical, with the highest possible severity score of 10.0.
- CVE-2021-45046: Similar to CVE-2021-44228, this enables a remote attacker to cause RCE, a denial-of-service (DoS) condition, or other effects in certain non-default configurations. This vulnerability affects all versions of Log4j from 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0. Patches for CVE-2021-44228 may not mitigate against this vulnerability and an additional patch may be required depending on the vendor. The CVSS rates this vulnerability as Critical, with a severity score of 9.0.
- CVE-2021-45105: Similar to CVE-2021-45046 but affecting Log4j versions 2.8.0 to 2.16.0, in some deployment scenarios. This vulnerability can allow a malicious actor to deliberately or inadvertently trigger a denial of service while attempting to obfuscate exploitation of CVE-2021-44228. The CVSS rates this vulnerability as High, with a severity score of 7.5.
- CVE-2021-44832: A vulnerability which allows an **attacker with control over Log4j configuration files** to download and execute a payload on non-default Log4j instances where the Java Database Connector (JDBC) Appender is used. This vulnerability affects all versions of Log4j from 2.0-alpha7 through 2.17.0, with exception of 2.3.2 and 2.12.4. The CVSS rates this vulnerability as Moderate, with a severity score of 6.6.

Given the current focus on Log4j by both the security research community and malicious actors, additional vulnerabilities may be discovered within Log4j. Australian organisations are strongly encouraged to remain aware of any emerging vulnerabilities and available patches.

Exploitation and Post-Exploitation Activities

The ACSC is aware of widespread scanning and reconnaissance activity against Australian organisations by malicious actors to identify the Log4j vulnerability. The ACSC has observed successful exploitation of the Log4j vulnerability and the compromise of systems and networks within Australia and globally, across all sectors of the economy.

An observed string substitution obfuscation technique which seeks to obscure exploitation of the remote code execution vulnerability can cause an infinite recursion resulting in a denial of service condition in versions of Log4j between 2.8.0 and 2.16.0.

The ACSC is also aware of reporting that malicious cyber actors have patched Log4j on systems after exploitation and compromise to avoid detection by security teams.

Given the widespread use of Log4j, patterns of post-exploitation activity are still emerging.

Mitigation and Detection Recommendations

Affected products

Australian organisations should check whether products they use or products developed in-house are affected by the Log4j vulnerability. The following links are helpful resources for identifying affected products:

- US Cybersecurity & Infrastructure Security Agency maintained community source list of publicly available information and vendor-supplied advisories regarding the Log4j vulnerability.
- The Netherlands National Cyber Security Centre list of affected products.

ACSC recommended prioritised mitigations

Individuals should **update all applications as soon as vendor patches become available.**

In accordance with the *Essential Eight (E8) – Patch Applications*, **organisations** should contact their vendors and **apply the latest patches immediately** where Log4j is known to be used. Upgrade to the current release of Log4j 2.17.1, which disables the vulnerable functionality and mitigates against the known string substitution denial of service condition.

Organisations should also **check internally developed or in-house software for use of Log4j** and upgrade to the latest version of Log4j (version 2.17.1 as of publication), and consider disabling the `JndiLookup` class. Organisations should limit use of remote files to configure Log4j instances, check for use of the JDBC Appender, and consider configuring the JDBC Appender to only use the JAVA protocol.

Software vendors should work to identify their use of the Log4j logging library in their products, and develop the required patches including the latest available version of Log4j to **assist their customers to remediate the vulnerability on their systems.**

Where upgrading is not possible, organisations should apply the hardening advice to disable the `JndiLookup` class. Please note that from version 2.17.1, the `log4j2.enableJndi` property has been refactored into three properties and support for the LDAP protocol has been removed for JNDI connections.

For software that organisations directly manage, mitigation advice on how to disable the JNDI points has been published in many places. A useful summary is in this post from Cloudflare.

As a last resort, **organisations** may implement network segmentation and segregation of affected hosts, noting that this presents only a partial mitigation for potential activity;

- Specifically for these vulnerabilities, configure network access rules to prevent vulnerable hosts from initiating requests to all JNDI related naming services;
- If practical, disable outbound connections from the vulnerable hosts to the internet, especially outbound Lightweight Directory Access Protocol (LDAP) and Domain Naming System (DNS) requests to untrusted networks;
- Isolate hosts running vulnerable applications to prevent lateral movement.

ACSC detection recommendations

Regardless of how quickly patches are applied, organisations should assume a malicious actor may have compromised their systems or networks, and take steps to continually monitor and investigate for indictors of exploitation and compromise.

The ACSC is also aware of reporting that malicious cyber actors have patched Log4j on systems after exploitation and compromise to avoid detection by security teams. Organisations should investigate instances of unexplained patching or recent modification of Log4j configuration files not undertaken by security teams.

As initial investigative activity, the ACSC recommends the following methods for detecting further malicious activity, on any system running Log4j.

- The Netherlands National Cyber Security Centre list of indicators of compromise
- Cisco Talos indicators of compromise

- Log4j remote code execution detection

Further Information

There are already useful open source information sources on Log4j vulnerability. For example:

- Log4Shell explained – how it works, why you need to know, and how to fix it – Naked Security (sophos.com) – provides a technical description of the vulnerability.
- Inside the Log4j2 vulnerability– provides mitigation advice.
- Digging deeper into Log4Shell – provides a semi-technical explanation of the exploit including a diagram.

The ACSC encourages organisations to verify if their software is vulnerable by actively monitoring vendor notifications or authoritative lists of known vulnerable software platforms.

Assistance / Where can I go for help?

The ACSC is monitoring the situation and is able to provide assistance and advice as required. Organisations that have been impacted or require assistance can contact the ACSC via 1300 CYBER1 (1300 292 371).