Texas Department of Information Resources Guidance on Log4j Vulnerability

TLP: WHITE

DATE: Dec 15, 2021 | Updated: Jan 7, 2022 **Version 4**

TLP: White - The materials provided are for information only. Any recommendations are offered solely for your consideration, to the extent applicable to your circumstances.

CRITICAL VULNERABILITY | Log4j | Java | Logging Library | DOS | RCE | InfoLeak

A series of critical vulnerabilities in Log4j have been widely publicized and are being actively exploited by threat actors. Texas DIR Office of the Chief Information Security Officer (OCISO) recommends all organizations evaluate their applications and services for the Log4j vulnerability and take immediate action to mitigate the vulnerability and update the affected library as quickly as possible.

BACKGROUND

In December 2021, multiple critical vulnerabilities in the open-source Java logging library, known as Log4j were disclosed. These vulnerabilities allowed for Remote Code Execution (RCE), Denial-of-Service (DoS), and other critical impacts.

IMPACTED VERSIONS

The original Log4j versions with the critical remote code execution vulnerability are **versions 2.0-beta9 to 2.14.1**. These versions were available from September 2013 until December 6, 2021. Additional vulnerabilities have been discovered in subsequent releases.

Organizations using Log4j should immediately upgrade to **Log4j 2.17.1 (Java 8), 2.12.4 (Java 7) or 2.3.2 (Java 6)**, as soon as possible.

The currently identified vulnerabilities are listed in the table below.

CVE	Score	Vulnerability Type	Affected Log4j Versions
CVE-2021-44228	10.0	Remote Code Execution	2.0-beta9 to 2.14.1
CVE-2021-45046	9.0	Information Leak and Remote Code Execution	2.0-beta9 to 2.15.0
CVE-2021-45105	7.5	Denial-of-Service	2.0-beta9 to 2.16.0
CVE-2021-4104	8.1	Untrusted Deserialization Flaw	1.2 (End of Life Aug 2015) Upgrade to 2.17.0
CVE-2021-44832	6.6	Remote Code Execution	Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4)

UPDATES AND MITIGATION

This section provides an overview of prioritizing upgrades, guidance for affected organizations, guidance for organizations using vendors affected by the vulnerability, and considerations for application developers.

PRIORITIZATION

The Cybersecurity and Infrastructure Security Agency (CISA) recommends that organizations running a vulnerable Log4j library prioritize patching of the vulnerability in the following order:

- Mission critical systems.
- Internet-facing systems, and networked servers.
- Other affected information technology and operational technology assets.

AFFECTED ORGANIZATIONS

CISA has identified immediate actions to protect against exploitation of the Log4j vulnerability. These actions are:

- Discover all internet facing assets that allow data inputs and use Log4j Java library anywhere in the environment.
- Discover all assets that use the Log4j library.
- Update or isolate affected assets. Assume compromise, identify common post-exploit sources and activity, and hunt for signs of malicious activity.
- Monitor for odd traffic patterns (e.g., JDNI LDAP/RMI outbound traffic, DMZ systems initiating outbound connections).

Organizations running products or applications with Log4j should implement the actions provided by CISA on the Log4j site and **upgrade to the current version** of Log4j as soon as possible.

For reference the CISA recommendations are included below.

- Apply available updates immediately, prioritizing updates based on the application's value and risk level.
    - Open-source vulnerability detection tools are available from several organizations and listed in the resources section.
    - These tools provide an initial evaluation as to whether the application is vulnerable to Log4Shell (CVE-2021-44228).
- Conduct a Security Review to search for signs of compromise, including a review of firewall logs and other security tools.
- Consider reporting compromises to CISA, the FBI, and the Texas Department of Information Resources (required via SPECTRIM for TAC 202 organizations, optional for other Texas organizations via the Texas ISAO threat report).

If organizations are unable to upgrade to a non-vulnerable version of Log4j or implement any mitigating or compensating controls, CISA recommends organizations remove the vulnerable Log4j software. Organizations should conduct a risk assessment and make a risk informed decision about removing vulnerable and unmitigated Log4j software.

VENDOR SERVICES

Use of the Log4j logging library is prevalent in consumer and enterprise applications, as such, the vendor community continues to update systems and software to mitigate the potential impacts of the vulnerability.

Organizations should evaluate their systems and monitor the vendor website and communications for instructions on updating systems to compensate for this vulnerability.

Several GitHub repositories are available to review vendors' vulnerability update statuses and recommended actions. Consider authoritative sources such as the CISA community-sourced GitHub repository. Additional GitHub sources are provided in the resources section.

MANAGED SERVICES PROVIDERS

Organizations that use an outsourced IT or cybersecurity provider, including an internal Security Operations Center (SOC), or a Managed Security Service Provider (MSSP), should ensure the service provide is aware of, monitoring, and taking appropriate actions on any Log4j references in the environment.

During discussion with the provider, consider requesting evidence of outbound traffic caused by Log4j exploitation attempts.

For additional guidance on working with a third party, review the CISA Insights for Risk Considerations for Managed Service Provider Customers.

RESOURCES

The following resources can support organizations as they mitigate and update systems in response to the Log4j vulnerability.

INFORMATIONAL

- CISA Guidance: https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
- CIS/MS-ISAC Log4j Zero-Day Vulnerability Response: https://www.cisecurity.org/log4j-zero-day-vulnerability-response/
- New Zealand Computer Emergency Response Team's Log4j Advisory: https://www.cert.govt.nz/it-specialists/advisories/log4j-rce-0-day-actively-exploited/

TECHNICAL

- Apache Log4j Security Vulnerabilities: https://logging.apache.org/log4j/2.x/security.html
- Swiss Government Computer Emergency Response Team Guidance: https://www.govcert.ch/blog/zero-day-exploit-targeting-popular-java-library-log4j/
- Dutch National Cyber Security Center – (Source for Log4j Indicators of Compromise IoCs): https://github.com/NCSC-NL/log4shell

REPORTED VENDOR LOG4J VULNERABILITIES

- GitHub - CISA Log4j Vulnerability Guidance: https://github.com/cisagov/log4j-affected-db
- GitHub – SwitHak: https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592
- GitHub - NCSC-NL: https://github.com/NCSC-NL/log4shell/tree/main/software

VULNERABILITY CHECKING TOOLS

- Huntress Log4shell Vulnerability Tester: https://log4shell.huntress.com/
- CERT Coordination Center Vulnerability Scanner: https://github.com/CERTCC/CVE-2021-44228_scanner
- Florian Roth's Log4j RCE Exploitation Detection: https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b
- NMAP Scripting Engine: https://github.com/Diverto/nse-log4shell
- FullHunt Log4j Vulnerability Tester: https://github.com/fullhunt/log4j-scan
- CISA Cyber Hygiene – Vulnerability Scanning: https://www.cisa.gov/uscert/resources/ncats#Cyber%20Hygiene

OPEN-SOURCE REPORTING

- Bleeping Computer - Latest Apache Log4j news

VERSION HISTORY

Version	Date	Notes
1.0	Dec 15, 2021	Initial Publication
2.0	Dec 18, 2021	Updated version recommendations, added CVEs section, additional resources added, updated CISA recommendations.
3.0	Dec 21, 2021	Updated resources, recommendations, and added considerations for organizations using managed service provides.
4.0	Dec 7, 2022	Update recommended versions and copy edits.