Mitigating Log4Shell and Other Log4j-Related Vulnerabilities

cisa.gov/uscert/ncas/alerts/aa21-356a

Summary

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), National Security Agency (NSA), Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), the Computer Emergency Response Team New Zealand (CERT NZ), the New Zealand National Cyber Security Centre (NZ NCSC), and the United Kingdom's National Cyber Security Centre (NCSC-UK) are releasing this joint Cybersecurity Advisory (CSA) to provide mitigation guidance on addressing vulnerabilities in Apache's Log4j software library: CVE-2021-44228 (known as "Log4Shell"), CVE-2021-45046, and CVE-2021-45105. Sophisticated cyber threat actors are actively scanning networks to potentially exploit Log4Shell, CVE-2021-45046, and CVE-2021-45105 in vulnerable systems. According to public reporting, Log4Shell and CVE-2021-45046 are being actively exploited.

CISA, in collaboration with industry members of CISA's Joint Cyber Defense Collaborative (JCDC), previously published guidance on Log4Shell for vendors and affected organizations in which CISA recommended that affected organizations immediately apply appropriate patches (or apply workarounds if unable to upgrade), conduct a security review, and report compromises to CISA or the FBI. CISA also issued an Emergency Directive directing U.S. federal civilian executive branch (FCEB) agencies to immediately mitigate Log4j vulnerabilities in solution stacks that accept data from the internet. This joint CSA expands on the previously published guidance by detailing steps that vendors and organizations with IT and/or cloud assets should take to reduce the risk posed by these vulnerabilities.

These steps include:

- Identifying assets affected by Log4Shell and other Log4j-related vulnerabilities,
- Upgrading Log4j assets and affected products to the latest version as soon as patches are available and remaining alert to vendor software updates, and
- Initiating hunt and incident response procedures to detect possible Log4Shell exploitation.

This CSA also provides guidance for affected organizations with operational technology (OT)/industrial control systems (ICS) assets.

Log4j is a Java-based logging library used in a variety of consumer and enterprise services, websites, applications, and OT products. These vulnerabilities, especially Log4Shell, are severe—Apache has rated Log4Shell and CVE-2021-45046 as critical and CVE-2021-45105

as high on the Common Vulnerability Scoring System (CVSS). These vulnerabilities are likely to be exploited over an extended period. CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK strongly urge all organizations to apply the recommendations in the Mitigations section.

CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK encourage leaders of organizations to review NCSC-UK's blog post, Log4j vulnerability: what should boards be asking?, for information on Log4Shell's possible impact on their organization as well as response recommendations.

Note: this is an evolving situation, and new vulnerabilities are being discovered. CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK will update this CSA as we learn more about this exploitation and have further guidance to impart.

Click here for a PDF version of this report.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, or NCSC-UK.

Technical Details

Log4Shell

Log4Shell, disclosed on December 10, 2021, is a remote code execution (RCE) vulnerability affecting Apache's Log4j library, versions 2.0-beta9 to 2.14.1. The vulnerability exists in the action the Java Naming and Directory Interface (JNDI) takes to resolve variables. Affected versions of Log4j contain JNDI features—such as message lookup substitution—that do not protect against adversary-controlled Lightweight Directory Access Protocol (LDAP), Domain Name System (DNS), and other JNDI-related endpoints.

An adversary can exploit Log4Shell by submitting a specially crafted request to a vulnerable system that causes that system to execute arbitrary code. The request allows the adversary to take full control over the system. The adversary can then steal information, launch ransomware, or conduct other malicious activity.

CVE-2021-45046

CVE-2021-45046, disclosed on December 13, 2021, 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. In response, Apache released Log4j version 2.16.0 (Java 8).

CVE-2021- 45105

CVE-2021-45105, disclosed on December 16, 2021, enables a remote attacker to cause a DoS condition or other effects in certain non-default configurations. According to Apache, when the logging configuration uses a non-default Pattern Layout with a Context Lookup (for example, `$${ctx:loginId}`), attackers with control over Thread Context Map (MDC) input data can craft malicious input data that contains a recursive lookup, resulting in a `StackOverflowError` that will terminate the process. In response, Apache released Log4j version 2.17.0 (Java 8).

Impact

Log4Shell and CVE-2021-45046—rated as critical vulnerabilities by Apache—are severe because Java is used extensively across IT and OT platforms, they are easy to exploit, and applying mitigations is resource intensive. Log4Shell is especially critical because it allows malicious actors to remotely run code on vulnerable networks and take full control of systems.

According to public reporting, exploitation of Log4Shell began on or around December 1, 2021, and a proof-of-concept exploit is publicly available for this vulnerability. The FBI has observed attempted exploitation and widespread scanning of the Log4j vulnerability to gain access to networks to deploy cryptomining and botnet malware. The FBI assesses this vulnerability may be exploited by sophisticated cyber threat actors and incorporated into existing cyber criminal schemes that are looking to adopt increasingly sophisticated obfuscation techniques. According to public reporting, CVE-2021-45046 is being actively exploited as well.

CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK assess that exploitation of these vulnerabilities, especially Log4Shell, is likely to increase and continue over an extended period. Given the severity of the vulnerabilities and likely increased exploitation, CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK strongly urge all organizations to apply the recommendations in the Mitigations section to identify, mitigate, and update affected assets.

For more information on these vulnerabilities, see the Apache Log4j Security Vulnerabilities webpage.

Mitigations

Vendors

CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK encourage vendors to:

1. **Immediately identify, mitigate, and update affected products** that use Log4j to the latest patched version.
    1. For environments using Java 8 or later, upgrade to Log4j version 2.17.0 (released December 17, 2021) or newer.
    2. For environments using Java 7, upgrade to Log4j version 2.12.3 (released December 21, 2021). **Note:** Java 7 is currently end of life and organizations should upgrade to Java 8.
2. **Inform your end users of products that contain these vulnerabilities** and strongly urge them to prioritize software updates. CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK strongly recommend vendors take steps to ensure messaging on software updates reaches the widest possible audience (for example, avoid placing relevant information behind paywalls). **Note:** CISA is actively maintaining a GitHub page and repository with patch information for products known to be affected by Log4Shell. CISA has also notified ICS vendors that may be affected and has asked them to confirm any assets affected by Log4Shell and to apply available mitigations.

Affected Organizations with IT and Cloud Assets

CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK recommend that affected organizations take the following steps to patch these vulnerabilities in their IT and cloud assets and initiate threat hunting to detect possible compromise. Organizations with OT/ICS environments should review the Organizations with OT/ICS Assets section for additional guidance. **Note:** this guidance includes resources that may or may not be possible for all organizations. CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK recommend that organizations apply the mitigations listed in this advisory to the extent allowed by their environments.

1. Identify vulnerable assets in your environment.

Knowing where Log4j and other affected products exist in your environment is key for protecting your networks.

1. **Inventory all assets that make use of the Log4j Java library.** According to public reporting, adversaries are patching and mitigating assets they compromise to retain control of assets. To avoid missing such defense evasion, organizations should carefully track assets under investigation.
    1. Assume all versions of Java and Log4j are vulnerable and include them in the inventory.
    2. Ensure the inventory includes all assets, including cloud assets, regardless of function, operating system, or make. Ensure the inventory includes the following information about each asset
        1. Software versions
        2. Timestamps of when last updated and by whom
        3. User accounts on the asset with their privilege level
        4. Location of asset in your enterprise topology
2. **Identify the inventoried assets that are likely vulnerable.**
    1. Use CISA's GitHub repository and CERT/CC's CVE-2021-44228_scanner to identify assets vulnerable to Log4Shell.

Additional resources for detecting vulnerable instances of Log4j are identified below. CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK will update the sources for detection rules as we obtain them. **Note:** due to the urgency to share this information, CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK have not yet validated this content.

- To identify server applications that may be affected by Log4Shell and CVE-2021-45046, see TrendMicro: Log4J Vulnerability Tester.
- For a list of hashes to help determine if a Java application is running a vulnerable version of Log4j, see:
    - Rob Fuller's GitHub page: CVE-2021-44228-Log4Shell-Hashes, and
    - The NCC Group's GitHub page: Cyber-Defence/Intelligence/CVE-2021-44228/.
- For PowerShell to detect vulnerable instances, see:
    - Nathan Kula's GitHub page: PowerShellSnippets/Invoke-Log4ShellScan.ps1, and
    - Will Dormann's GitHub page: checkjndi.ps1.
- For guidance on using Canary Token to test for callback, see Thinkst Canary's Twitter thread on using Canary Tokens.
- For guidance on using Burpsuite Pro to scan, see:
    - Silent Signal's GitHub page: burp-log4shell, and
    - PortSwigger's GitHub page: active-scan-plus-plus.
- For guidance on using NetMap's Nmap Scripting Engine (NSE), see Divertor's GitHub page: nse-log4shell.
- See Florian Roth's GitHub page, Fenrir 0.9.0 - Log4Shell Release, for guidance on using Roth's Fenrir tool to detect vulnerable instances.

2. Mitigate known and suspected vulnerable assets in your environment.

A. **Treat known and suspected vulnerable assets** as compromised. These assets should be isolated until they are mitigated and verified (step 2.D). The method of isolation that you should use depends on the criticality of the asset. Possible isolation methods include:

- Physically removing the asset from the network (e.g., unplug the network cable);
- Moving the asset to a "jail VLAN" with heightened monitoring and security;
- Blocking at the network layer (a switch or some other device);
- Implementing a firewall (including web application firewall) with strict port control and logging; or
- Restricting the asset's communication, especially to the internet and the rest of the enterprise network.

B. **Patch Log4j and other affected products to the latest version.**

- See the Apache Log4j Security Vulnerabilities webpage (as of December 22, 2021, the latest Log4j version is 2.17.0 for Java 8 and 2.12.3 for Java 7). **Note:** patching or updating Java is not enough, you must upgrade the Log4j library itself.
- For other affected products, see CISA's GitHub page.

Note: if your organization is unable to immediately identify and patch vulnerable instances of Log4j, apply appropriate workarounds. CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK recommend using vendor-provided mitigations when available. Due to the rapidly evolving situation, these workarounds should not be considered permanent fixes and organizations should apply the appropriate patch as soon as it is made available. Additional mitigations are identified below; however, organizations should use these mitigations at their own risk as they may be incomplete, temporary, or cause harmful effects, such as application instability, a DoS condition, or log evasion.

- Remove the `Jndilookup.class` from the class path. [1]
- Delete or rename `Jndilookup.class`. **Note:** removal of the `JndiManager` will cause the `JndiContextSelector` and `JMSAppender` to no longer function). [2]
- Apply a hot patch.
  - NCC Group: log4j-jndi-be-gone: A simple mitigation for CVE-2021-44228
  - Amazon AWS:
    - GitHub page: hotpatch-for-apache-log4j2
    - Blog: Hotpatch for Apache Log4j

C.**Keep an inventory of known and suspected vulnerable assets and what is done with them throughout this process.** It is important to track patching because malicious cyber actors may compromise an asset and then patch it to protect their operations. Organizations should keep a meticulous record of vulnerable assets they have patched to identify whether a threat actor may have patched an asset.

D. **Verify the mitigation has worked,** if possible.

1. Scan the patched/mitigated asset with the tools and methods listed in step 1.B. Use more than one method to verify the mitigation was successfully applied.
2. Monitor the asset closely.
3. Remain alert to changes from vendors for the software on the asset. Additionally, see CISA's GitHub page for known affected products and patch information. CISA will continually update the repository as vendors release patches.

3. Initiate hunt and incident response procedures. Given the widespread exploitation of this vulnerability, CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK encourage all organizations to assume their assets that use Log4j may have been compromised and initiate hunt procedures.

A. **Hunt for signs of exploitation and compromise.**

1. Treat assets that use Log4j as suspect and conduct vigorous forensic investigation of those assets.
2. Inspect and monitor accounts across your enterprise that exist on or connect to assets that use Log4j.
3. Inspect changes to configurations made since December 1, 2021, and verify they were intended, especially on assets that use Log4j.
4. Use CISA's GitHub page to detect possible exploitation or compromise.

Additional resources to detect possible exploitation or compromise are identified below. **Note:** due to the urgency to share this information, CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK have not yet validated this content.

- Cisco Talos blog: Threat Advisory: Critical Apache Log4j vulnerability being exploited in the wild
- Curated Intelligence GitHub page: Log4Shell-IOCs (**Note:** Curated Intelligence notes that the "IOCs shared by these feeds are low-to-medium confidence we [Curated Intelligence] strongly recommend not adding them to a blocklist.")
- EmergingThreat.net: signatures to assist with detection of CVE-2021-44228 activity
- Florian Roth's GitHub pages:
  - Log4j RCE Exploitation Detection
  - signature-base/yara/expl_log4j_cve_2021_44228.yar
  - log4shell-detector
- Huntress blog: Critical RCE Vulnerability: log4j - CVE-2021-44228
- Mandiant blog: Now You Serial, Now You Don't – Systematically Hunting for Deserialization Exploits
- Microsoft Security Response Center: Microsoft's Response to CVE-2021-44228 Apache Log4j 2
- NCC Group: Log4Shell: Reconnaissance and post exploitation network detection

- Sigma GitHub pages:
  - sigma/rules/web/web_cve_2021_44228_log4j.yml
  - sigma/rules/web/web_cve_2021_44228_log4j_fields.yml

B. **If compromise is detected, organizations should:**

1. Initiate incident response procedures. See the joint advisory from ACSC, CCCS, NZ NCSC, CERT NZ, NCSC-UK, and CISA on Technical Approaches to Uncovering and Remediating Malicious Activity for guidance on hunting or investigating a network, and for common mistakes in incident handling. CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK encourage organizations to see CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. Although tailored to U.S. FCEB agencies, these playbooks provide operational procedures for planning and conducting cybersecurity incident and vulnerability response activities and detail each step for both incident and vulnerability response.
2. Consider reporting compromises immediately to applicable cybersecurity authorities. Organizations are encouraged to be as thorough as possible by including information such as IP addresses/domains used to exploit your infrastructure, exploited applications/servers, administrators contact information, and the start and end dates of the attack.

- U.S. organizations should report compromises to CISA and the FBI.
- Australian organizations can visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents.
- Canadian organizations can report incidents by emailing CCCS at contact@cyber.gc.ca.
- New Zealand organizations can visit NCSC.govt.nz to report incidents.
- UK organizations can report a significant cyber security incident at ncsc.gov.uk/report-an-incident (monitored 24 hrs) or, for urgent assistance, call 03000 200 973.

4. Evaluate and apply other mitigations.

A. **Remain alert to changes from vendors for the software on the asset, and immediately apply updates to assets** when notified by a vendor that their product has a patch for this vulnerability. Additionally, see CISA's GitHub repository for known affected products and patch information. CISA will continually update the repository as vendors release patches.

B. **Continue to monitor Log4J assets closely.** Continually use signatures and indicators of compromise that may indicate exploitation.

1. See the exploitation and detection resources listed in step 3.A.(4).
2. Be aware that there are many ways to obfuscate the exploit string. Do not depend on one detection method to work all the time.

C. **Continue to monitor the Apache Log4j Security Vulnerabilities webpage for new updates. Note:** as this is an evolving situation and new vulnerabilities in Log4J are being discovered, organizations should ensure their Apache Log4j is up to date. Identify the software your enterprise uses and stay on top of updates as these may be superseded by other updates and fixes.

D. **Block specific outbound Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) network traffic.**

1. **Outbound LDAP:** for most networks, LDAP is used internally, but it is rare for LDAP requests to be routed outside a network. Organizations should block outbound LDAP or use an allowlist for outbound LDAP to known good destinations. **Note:** this may be difficult to detect on certain ports without a firewall that does application layer filtering.
2. **Remote Method Invocation (RMI):** for most networks, RMI is either unused or used for internal sources. Organizations should block outbound RMI or use an allowlist for outbound RMI to known good destinations.
3. **Outbound DNS:** organizations using enterprise DNS resolution can block outbound DNS from sources other than identified DNS resolvers. At a minimum, blocking direct outbound DNS from web application servers configured to use enterprise DNS resolution will mitigate the risks to those systems.

Note: blocking attacker internet IP addresses during this event is difficult due to the high volume of scanning from non-malicious researchers and vendors. The false positives on IP addresses are high. Organizations should focus on looking for signs of successful exploitation and not scans.

Affected Organizations with OT/ICS Assets

Due to the pervasiveness of the Apache Log4j software library—and the integration of the library in operational products—CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK strongly recommend that OT asset owners and operators review their operational architecture and enumerate the vulnerability status against current product alerts and advisories. If a product does not have a security advisory specifically addressing the status of the vulnerability, treat it with additional protections. CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK urge patching or deployment of mitigations to reduce the risk of the threat of these vulnerabilities.

Note: CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK recommend prioritizing patching IT devices, especially those with internet connectivity. Affected internet-facing devices as well as laptops, desktops, and tablets are especially susceptible to exploitation of these vulnerabilities. OT/ICS devices—if segmented appropriately from the IT environment—do not face the internet and, as such, have a smaller attack surface to this vulnerability. Exploitation of IT devices may affect OT/ICS devices if there is insufficient network segmentation that prevents lateral movement.

CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK recommend that OT/ICS asset owner/operators take the following guidance into consideration:

1. **Review operational architecture and enumerate the vulnerability against current product alerts and advisories.** If products do not have a security advisory specifically addressing their status of the vulnerability, it is recommended to treat these devices with additional protections.
2. **Implement the steps listed in the previous section to identify and isolate vulnerable assets** in the OT/ICS environment. Understand what type of products in the OT environment would be affected. Many OT/ICS-specific products incorporate vulnerable versions of the Log4j library.
3. **Use a risk-informed decision-making process to apply the latest version of hotfixes or patches** to affected devices as soon as is operationally feasible. If patches cannot be applied, mitigations provided by the product's manufacturer or reseller should be deployed. **Note:** CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK recommend, as quality assurance, that users test the update in a test development environment that reflects their production environment prior to installation.
4. **Minimize network exposure for all control system devices and/or systems**, and ensure they are not accessible from the internet.
5. **Locate control system networks and remote devices behind firewalls and isolate them** from the business network.

When remote access is required, use secure methods such as virtual private networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that a VPN is only as secure as its connected devices.

CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK also remind organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing any suspected malicious activity should follow their established internal procedures and consider reporting compromises immediately.

- U.S. organizations should report compromises to CISA and the FBI.
- Australian organizations can visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents.
- Canadian organizations can report incidents by emailing CCCS at contact@cyber.gc.ca.
- New Zealand organizations can visit NCSC.govt.nz to report incidents.
- UK organizations can report a significant cyber security incident at ncsc.gov.uk/report-an-incident (monitored 24 hrs) or, for urgent assistance, call 03000 200 973.

Resources

For more information, resources, and general guidance, including resources and mitigation guidance from industry members of JCDC, see CISA's webpage Apache Log4j Vulnerability Guidance. **Note:** due to the prominent and ever evolving nature of this vulnerability, there are multiple unverified published guidance documents that are geared towards Log4j vulnerabilities. CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK encourage all organizations to verify information with trusted sources, such CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, NCSC-UK vendors.

References

Revisions

December 22, 2021: Initial Version

December 23, 2021: Updated Resource URL

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.