Software Engineering Institute

CERT Coordination Center

Home | Notes | Search | Report a Vulnerability

Home › Notes › VU#930724

Apache Log4j allows insecure JNDI lookups

Vulnerability Note VU#930724

Original Release Date: 2021-12-15 | Last Revised: 2022-02-07

Overview

Apache Log4j allows insecure JNDI lookups that could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the vulnerable Java application using Log4j.

CISA has published Apache Log4j Vulnerability Guidance and provides a Software List.

Description

The default configuration of Apache Log4j supports JNDI (Java Naming and Directory Interface) lookups that can be exploited to exfiltrate data or execute arbitrary code via remote services such as LDAP, RMI, and DNS.

This vulnerability note includes information about the following related vulnerabilities.

ABOUT VULNERABILITY NOTES

CONTACT US ABOUT THIS VULNERABILITY

PROVIDE A VENDOR STATEMENT

- CVE-2021-44228 tracks the initial JNDI injection and RCE vulnerability in Log4j 2. This vulnerability poses considerabily more risk than the others.
- CVE-2021-4104 tracks a very similar vulnerability that affects Log4j 1 if JMSAppender and malicious connections have been configured.
- CVE-2021-45046 tracks an incomplete fix for CVE-2021-44228 affecting Log4j 2.15.0 when an attacker has "...control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern."

We provide tools to scan for vulnerable jar files.

More information is available from the Apache Log4j Security Vulnerabilities page, including these highlights.

Certain conditions must be met to make Log4j 1.x vulnerable:

> Log4j 1.x mitigation: Log4j 1.x does not have Lookups so the risk is lower. Applications using Log4j 1.x are only vulnerable to this attack when they use JNDI in their configuration. A separate CVE (CVE-2021-4104) has been filed for this vulnerability. To mitigate: audit your logging configuration to ensure it has no JMSAppender configured. Log4j 1.x configurations without JMSAppender are not impacted by this vulnerability.

Log4j API code alone is not affected:

> Note that only the log4j-core JAR file is impacted by this vulnerability. Applications using only the log4j-api JAR file without the log4j-core JAR file are not impacted by this vulnerability.

Impact

A remote, unauthenticated attacker with the ability to log specially crafted messages can cause Log4j to connect to a service controlled by the attacker to download and execute arbitrary code.

Solution

In Log4j 2.12.2 (for Java 7) and 2.16.0 (for Java 8 or later) the message lookups feature has been completely removed. In addition, JNDI is disabled by default and other default configuration settings are modified to mitigate CVE-2021-44228 and CVE-2021-45046.

For Log4j 1, remove the JMSAppender class or do not configure it. Log4j 1 is not supported and likely contains unfixed bugs and vulnerabilities (such as CVE-2019-17571).

For applications, services, and systems that use Log4j, consult the appropriate vendor or provider. See the CISA Log4j Software List and the Vendor Information section below.

Workarounds

Remove the JndiLookup class from the classpath, for example:

```
zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
```

As analysis has progressed, certain mitigations have been found to be less effective or incomplete. See "Older (discredited) mitigation measures" on the Apache Log4j Security Vulnerabilities page.

SLF4J also recommends write-protecting Log4j configuration files.

Acknowledgements

Apache credits Chen Zhaojun of Alibaba Cloud Security Team for reporting CVE-2021-44228 and CVE-2021-4104 and Kai Mindermann of iC Consult for CVE-2021-45046.

Much of the content of this vulnerability note is derived from Apache Log4j Security Vulnerabilities and http://slf4j.org/log4shell.html.

This document was written by Art Manion.

Vendor Information

Filter by status:

Filter by content:

Sort by:

All

☐ 📢 Additional information available

Status

Expand all

📢	ABB	Affected
📢	Adobe	Affected
📢	ADTRAN	Affected
📢	Amazon	Affected
📢	Apache Commons	Affected
📢	Apache Solr	Affected
📢	Apache Spark	Affected
📢	Apache Struts	Affected
📢	Apache Tomcat	Affected
📢	Apereo	Affected

View all 1643 vendors ⌄

References

- https://github.com/CERTCC/CVE-2021-44228_scanner
- https://logging.apache.org/log4j/2.x/security.html#Fixed_in_Log4j_2.15.0
- https://logging.apache.org/log4j/2.x/security.html#Fixed_in_Log4j_2.16.0
- https://issues.apache.org/jira/browse/LOG4J2-3201
- https://issues.apache.org/jira/browse/LOG4J2-3198
- https://github.com/apache/logging-log4j2/pull/607
- https://github.com/apache/logging-log4j2/pull/608
- https://lists.apache.org/thread/gzj2jsglvsffzs8zormxyly0vofdxp6j

- https://lists.apache.org/thread/4gl0cg87hyp5n8kf61q11sy446y3lw7v
- http://slf4j.org/log4shell.html
- https://www.cve.org/CVERecord?id=CVE-2021-44228
- https://lists.apache.org/thread/0x4zvtq92yggdgvwfgsftqrj4xx5w0nx
- https://www.cve.org/CVERecord?id=CVE-2021-4104
- https://www.cve.org/CVERecord?id=CVE-2021-45046
- http://www.slf4j.org/log4shell.html
- https://www.cisa.gov/news/2021/12/11/statement-cisa-director-easterly-log4j-vulnerability
- https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
- https://github.com/cisagov/log4j-affected-db
- https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability
- https://research.nccgroup.com/2021/12/12/log4j-jndi-be-gone-a-simple-mitigation-for-cve-2021-44228/
- https://www.veracode.com/blog/security-news/urgent-analysis-and-remediation-guidance-log4j-zero-day-rce-cve-2021-44228
- https://www.lunasec.io/docs/blog/log4j-zero-day/

Other Information

CVE IDs:	CVE-2021-4104 CVE-2021-44228 CVE-2021-45046
Date Public:	2021-12-15
Date First Published:	2021-12-15
Date Last Updated:	2022-02-07 13:29 UTC
Document Revision:	76

Sponsored by CISA.

Download PGP Key

Read CERT/CC Blog

Learn about Vulnerability Analysis

Carnegie Mellon University
Software Engineering
Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
412-268-5800

Contact SEI

Contact CERT/CC

☎ 412-268-5800
✉ cert@cert.org