Security Bulletin 2021-1

Log4Shell vulnerability

Publication date :	16/12/2021
Last update :	07/01/2022
Document revision :	1.0 Rev C
Content of the document :	This document contains information about vulnerabilities affecting the Log4j Apache library dubbed Log4Shell.

Overview

This security bulletin follows an alert released on December 10th 2021 and related to the newly discovered Log4j Apache library vulnerability dubbed Log4Shell.
ARC Informatique invites all users of its products to actively watch for software and hardware updates addressing Log4Shell. It is advised to test them prior to deployment on production system. Such tests should cover effectiveness, performances and regressions.

Affected products and components

ARC Informatique's products are NOT affected by this vulnerability, therefore no update is required. The library Log4j is not used or included in any supported or unsupported release of our products.

At the time of writing, no third-party product distributed by ARC Informatique is known to be affected.

Nevertheless, the hosting environment and network components might be affected and require close attention and careful inspection. Security updates will be necessary for products and services using affected versions of Log4j. We recommend you to refer to vendors of these products and services.

Timeline

On November 24th 2021, Apache teams were notified of a Remote Code Execution vulnerability affecting the Log4j library by the Alibaba Cloud security team.

On December 6th 2021, version 2.15.0 of the Log4j library has been released to fix this vulnerability. The library being widely used, it still requires to be deployed in the affected products and services to be updated.

On December 9th 2021, a first Proof Of Concept was posted on GitHub.

On December10th 2021, NIST officially published the new CVE-2021-44228 and since then, this vulnerability has been massively exploited.

On December 13th 2021, version 2.16.0 of the Log4j library has been released with complementary fixes related to a new vulnerability resulting in a Denial Of Service attack.

On December 14th 2021, NIST officially published the new CVE-2021-45046.

On December 18th 2021, version 2.17.0 of the Log4j library has been released with a complementary fixe related to a new vulnerability resulting in another Denial Of Service attack. NIST officially published the associated CVE-2021-45105.

On December 27th 2021, version 2.17.1 of the Log4j library has been released with complementary fixes related to a vulnerability resulting in a Remote Code Execution attack.

On December 28th, NIST officially publish the new CVE-2021-44832.

Vulnerability details

1. Remote Code Execution

CVE-IDS	CVE-2021-44228
Publication date	2021.12.10
Description	Apache Log4j2 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0, this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.
Impact	Remote execution of an arbitrary process
CVSS v3.1 Base Score	10.0
Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Exploitability	Remote~~/Local~~
Difficulty	Low/~~Medium/High~~
User interaction	None~~/Yes~~

2. Remote Code Excecution

CVE-IDS	CVE-2021-45046
Publication date	2021.12.14
Description	It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allows attackers with 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 (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments. Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for message lookup patterns and disabling JNDI functionality by default.
Impact	Remote Code Execution
CVSS v3.1 Base Score	9.0
Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
Exploitability	Remote~~/Local~~
Difficulty	~~Low/Medium~~/High
User interaction	None~~/Yes~~

3. Denial Of Service

CVE-IDS	CVE-2021-45105
Publication date	2021.12.18
Description	Apache Log4j2 versions 2.0-alpha1 through 2.16.0 (excluding 2.12.3) did not protect from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial of service when a crafted string is interpreted. This issue was fixed in Log4j 2.17.0 and 2.12.3.
Impact	Denial of service
CVSS v3.1 Base Score	7.5
Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Exploitability	Remote~~/Local~~
Difficulty	Low/~~Medium/High~~
User interaction	None~~/Yes~~

4. Remote Code Excecution

CVE-IDS	CVE-2021-44832
Publication date	2021.12.28
Description	Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.
Impact	Remote Code Execution
CVSS v3.1 Base Score	6.6
Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H
Exploitability	Remote~~/Local~~
Difficulty	~~Low/Medium~~/High
User interaction	None~~/Yes~~

Immediate risk mitigation

1) The current exploits require making a connection to a remote system (attacker controlled). If possible, configure firewall outbound rules to block LDAP and RMI traffic.

2) Make an inventory of the impacted software and hardware assets, and if possible isolate or shut them down until a remediation solution is applied.

3) As soon as possible, apply vendor patches to impacted software and hardware, and update configuration according to their recommendations.

4) If your solution was internally developed, upgrade the Log4j library to its latest version.

References

The public ARC Informatique security alert page: www.pcvuesolutions.com
This security bulletin on the Technical Resources web site
CVE: CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832
Apache Log4j advisories: CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832
CERT-FR advisory: CERTFR-2021-ALE-022
CISA: Apache Log4j Vulnerability Guidance

Third-party products:
- Alert: ALERT software not affected by the LOG4J flaw
- DreamReport: FAQ 040: Does the log4j vulnerability impact Dream Reports?
- Moxa: Moxa's Response Regarding the Apache Log4j Vulnerability
- OPC UA Gateway: Log4Shell Attack Exploit

Want to report a vulnerability or provide feedback – Please email us at secure@arcinfo.com

Document history

Revision	Action	Date
Version 1.0	First publication	16/12/2021
Version 1.0 Rev A	Timeline and details updated with CVE-2021-45105	20/12/2021
Version 1.0 Rev B	Content of CVE-2021-45046 & CVE-2021-45105 updated	21/12/2021
Version 1.0 Rev C	References links for third-party products added Timeline and details updated with CVE-2021-44832	07/01/2022

ARC Informatique
Private limited company
capitalized
at 1 250 000 €
RCS Nanterre B 320 695 356
APE 5829C
SIREN 320 695 356
VAT N°FR 19320695356

Security Bulletin 2021-1

ISO 9001 and ISO 14001 certified

ARC Informatique

Headquarters and Paris offices
2 avenue de la Cristallerie
92310 Sèvres - France

tel + 33 1 41 14 36 00
fax + 33 1 46 23 86 02
hotline +33 1 41 14 36 25
arcnews@arcinfo.com
www.pcvuesolutions.com

We would love to hear your thoughts and suggestions
so we can improve this document
Contact us at secure@pcvuesolutions.com