



Apache Log4j JSON Template Layout: Improper serialization of non-finite floating-point values in JsonTemplateLayout

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-34481
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-10 16:16:31 UTC
Updated	2026-04-13 15:02:06 UTC
Description	Apache Log4j's JsonTemplateLayout https://logging.apache.org/log4j/2.x/manual/json-template-layout.html , in versions up

Risk And Classification

Primary CVSS: v4.0 6.3 MEDIUM from security@apache.org

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.001190000 probability, percentile 0.308590000 (date 2026-04-15)

Problem Types: CWE-116 | CWE-116 CWE-116 Improper Encoding or Escaping of Output

Version	Source	Type	Score	Severity	Vector
4.0	security@apache.org	Secondary	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache Log4j JSON Template Layout	affected 2.14.0 2.25.4 maven	Not specified
CNA	Apache Software Foundation	Apache Log4j JSON Template Layout	affected 3.0.0-alpha1 3.0.0-beta3 maven	Not specified

References

Reference	Source	Link	Tags
logging.apache.org/security.html	security@apache.org	logging.apache.org	
logging.apache.org/log4j/2.x/manual/json-template-layout.html	security@apache.org	logging.apache.org	
logging.apache.org/cyclonedx/vdr.xml	security@apache.org	logging.apache.org	
github.com/apache/logging-log4j2/pull/4080	security@apache.org	github.com	
www.openwall.com/lists/oss-security/2026/04/10/10	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
lists.apache.org/thread/n34zdv00gbkdbzt2rx9rf5mqz6lhpcv	security@apache.org	lists.apache.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

Vendor Comments And Credit

Discovery Credit

CNA: Ap4sh (Samy Medjahed) and Ethicxz (Eliott Laurie) (en)

Additional Advisory Data

Source	Time	Event
--------	------	-------

CNA	2026-02-16T18:14:00.000Z	Vulnerability reported by Ap4sh and ethicxz
CNA	2026-03-10T20:42:00.000Z	Candidate patch internally shared by Piotr P. Karwasz
CNA	2026-03-24T23:06:00.000Z	Fix shared publicly by Piotr P. Karwasz as pull request #4080
CNA	2026-03-25T09:54:00.000Z	Fix verified by the reporter
CNA	2026-03-28T11:19:00.000Z	Log4j 2.25.4 released

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)