Apache Log4j Core: verifyHostName attribute silently ignored in TLS configuration, allowing hostname verification bypass

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-34477
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-10 16:16:30 UTC
Updated	2026-04-10 16:16:30 UTC
Description	The fix for CVE-2025-68161 https://logging.apache.org/security.html#CVE-2025-68161 was incomplete: it addressed hostn

Risk And Classification

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

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-297 | CWE-297 CWE-297 Improper Validation of Certificate with Host Mismatch

Version	Source	Type	Score	Severity	Vector
4.0	security@apache.org	Secondary	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:L/SA:N/E:X
4.0	CNA	CVSS	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:L/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/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/MSC:X/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 Core	affected 2.12.0 2.25.4 maven	Not specified
CNA	Apache Software Foundation	Apache Log4j Core	affected 3.0.0-alpha1 3.0.0-beta3 maven	Not specified

References

Reference	Source	Link	Tags
lists.apache.org/thread/lkx8cl46t2bvkcwfcb2pd43ygc097lq4	security@apache.org	lists.apache.org	
github.com/apache/logging-log4j2/pull/4075	security@apache.org	github.com	
logging.apache.org/security.html	security@apache.org	logging.apache.org	
logging.apache.org/cyclonedx/vdr.xml	security@apache.org	logging.apache.org	
logging.apache.org/log4j/2.x/manual/appenders/network.html	security@apache.org	logging.apache.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Samuli Leinonen (original reporter) (en)

CNA: Naresh Kandula (independently) (en)

CNA: Vitaly Simonovich (independently) (en)

CNA: Raijuna (independently) (en)

CNA: Danish Siddiqui (djvirus, independently) (en)

CNA: Markus Magnuson (independently) (en)

CNA: Haruki Oyama (Waseda University, independently) (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-12-20T19:05:00.000Z	Vulnerability reported by Samuli Leinonen
CNA	2025-12-30T22:57:00.000Z	Candidate patch shared internally by Piotr P. Karwasz
CNA	2026-02-25T19:35:00.000Z	Independent report received from Naresh Kandula
CNA	2026-03-01T23:01:00.000Z	Independent report received from Vitaly Simonovich
CNA	2026-03-02T06:31:00.000Z	Independent report received from Raijuna
CNA	2026-03-08T18:17:00.000Z	Independent report received from Danish Siddiqui
CNA	2026-03-19T09:46:00.000Z	Independent report received from Markus Magnuson
CNA	2026-03-21T11:13:00.000Z	Independent report received from Haruki Oyama
CNA	2026-03-24T19:46:00.000Z	Fix shared publicly by Piotr P. Karwasz as pull request #4075
CNA	2026-03-28T11:19:00.000Z	Log4j 2.25.4 released

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