



Apache HTTP Server: mod_proxy_ajp: Heap Buffer Over-Read Due to Missing Null-Termination Check (ajp_msg_get_string)

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

Summary

CVE	CVE-2026-34032
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 14:16:33 UTC
Updated	2026-05-04 20:25:47 UTC
Description	Improper Null Termination, Out-of-bounds Read vulnerability in Apache HTTP Server. This issue affects Apache HTTP Ser

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from ADP

CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Problem Types: CWE-125 | CWE-170 | CWE-170 CWE-170 Improper Null Termination | CWE-125 CWE-125 Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache HTTP Server	affected 2.4.66 semver	Not specified

References

Reference	Source	Link	Tags
httpd.apache.org/security/vulnerabilities_24.html	security@apache.org	httpd.apache.org	Vendor Advisory
www.openwall.com/lists/oss-security/2026/05/04/16	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	Mailing List, Third Party
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: Tianshuo Han (<hantianshuo233@gmail.com>) (en)

CNA: Jérôme Djouder (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-01T02:27:00.000Z	Report received
CNA	2026-05-04T12:00:00.000Z	fixed in 2.4.x by r1933343

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

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