



Apache HTTP Server: multiple modules: HTTP response splitting forwarding malicious status line

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

Summary

CVE	CVE-2026-33523
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 15:16:04 UTC
Updated	2026-05-04 20:21:15 UTC
Description	HTTP response splitting vulnerability in multiple Apache HTTP Server modules with untrusted or compromised backend ser

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from ADP

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

Problem Types: CWE-443 | NVD-CWE-Other | CWE-443 CWE-443: HTTP response splitting

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/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 2.4.0 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/2026/05/04/23	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: Haruki Oyama (Waseda University) (en)

CNA: Merih Mengisteab (en)

CNA: Dawit Jeong (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-05T12:00:00.000Z	reported
CNA	2026-05-04T12:00:00.000Z	2.4.67 released
CNA	2026-05-04T12:00:00.000Z	fixed in 2.4.x by r1933360

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