Apache HTTP Server: http2: double free and possible RCE on early reset

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

Summary

CVE	CVE-2026-23918
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 15:16:03 UTC
Updated	2026-05-04 20:24:58 UTC
Description	Double Free and possible RCE vulnerability in Apache HTTP Server with the HTTP/2 protocol. This issue affects Apache H

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from ADP

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

EPSS: 0.000610000 probability, percentile 0.187650000 (date 2026-05-05)

Problem Types: CWE-415 | CWE-415 CWE-415 Double Free

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

vailability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	2.4.66	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/2026/05/04/19	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	Mailing List, Third P
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: Bartlomiej Dmitruk, striga.ai (en)

CNA: Stanislaw Strzalkowski, isec.pl (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-12-10T14:02:00.000Z	reported in PR 69899
CNA	2025-12-11T14:03:00.000Z	fixed in r1930444, r1930796

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report