fastify vulnerable to Body Schema Validation Bypass via Leading Space in Content-Type Header

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

Summary

CVE	CVE-2026-33806
State	PUBLISHED
Assigner	openjs
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-15 04:17:36 UTC
Updated	2026-04-17 15:49:28 UTC
Description	Impact: Fastify applications using schema.body.content for per-content-type body validation can have validation bypassed e

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from ce714d77-add3-4f53-aff5-83d477b104bb

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

EPSS: 0.000610000 probability, percentile 0.189790000 (date 2026-04-20)

Problem Types: CWE-1287 | CWE-1287 CWE-1287: Improper Validation of Specified Type of Input

Version	Source	Type	Score	Severity	Vector
3.1	ce714d77-add3-4f53-aff5-83d477b104bb	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

High

vailability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fastify	Fastify	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Fastify	Fastify	affected 5.3.2 5.8.5 semver	Not specified
CNA	Fastify	Fastify	unaffected 5.8.5 semver	Not specified

References

Reference	Source	Link	Tags
cna.openjsf.org/security-advisories.html	ce714d77-add3-4f53-aff5-83d477b104bb	cna.openjsf.org	Vendor
github.com/fastify/fastify/security/advisories/GHSA-mg2h-6x62-wpwc	ce714d77-add3-4f53-aff5-83d477b104bb	github.com	Not App
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

Vendor Comments And Credit

Discovery Credit

CNA: mcollina (en)

CNA: climba03003 (en)

CNA: jsumners (en)

CNA: UlisesGascon (en)

CNA: Vyntral (en)

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 registred 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