@fastify/reply-from vulnerable to connection header abuse enabling stripping of proxy-added headers

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

Summary

CVE	CVE-2026-33805
State	PUBLISHED
Assigner	openjs
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-15 11:16:34 UTC
Updated	2026-04-17 15:09:46 UTC
Description	@fastify/reply-from v12.6.1 and earlier and @fastify/http-proxy v11.4.3 and earlier process the client's Connection header a

Risk And Classification

Primary CVSS: v4.0 9 CRITICAL from ce714d77-add3-4f53-aff5-83d477b104bb

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:N/SC:L/SI:H/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

EPSS: 0.000420000 probability, percentile 0.126870000 (date 2026-04-20)

Problem Types: CWE-644 | CWE-644 CWE-644: Improper Neutralization of HTTP Headers for Scripting Syntax

Version	Source	Type	Score	Severity	Vector
4.0	ce714d77-add3-4f53-aff5-83d477b104bb	Secondary	9	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA
4.0	CNA	CVSS	9	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

None

Confidentiality

None

Integrity

High

Availability

None

Sub Conf.

Low

Sub Integrity

High

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:N/SC:L/SI:H/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	@fastifyreply-from	@fastify/reply-from	affected 12.6.2 semver	Not specified
CNA	@fastifyreply-from	@fastify/reply-from	unaffected 12.6.2 semver	Not specified
CNA	@fastifyreply-from	@fastify/http-proxy	affected 11.4.4 semver	Not specified
CNA	@fastifyreply-from	@fastify/http-proxy	unaffected 11.4.4 semver	Not specified

References

Reference	Source	Link	Ta
cna.openjsf.org/security-advisories.html	ce714d77-add3-4f53-aff5-83d477b104bb	cna.openjsf.org	
github.com/fastify/fastify-reply-from/security/advisories/GHSA-gwhp-pf74...	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

Vendor Comments And Credit

Discovery Credit

CNA: FredKSchott (en)

CNA: mcollina (en)

CNA: UlisesGascon (en)

CNA: climba03003 (en)

There are currently no legacy OID mappings associated with this CVE

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**