



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

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

## Summary

<b>CVE</b>	CVE-2026-33805
<b>State</b>	PUBLISHED
<b>Assigner</b>	openjs
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-15 11:16:34 UTC
<b>Updated</b>	2026-04-17 15:09:46 UTC
<b>Description</b>	@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/MSX/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/MSX/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	Tags
cna.openjsf.org/security-advisories.html	ce714d77-add3-4f53-aff5-83d477b104bb	<a href="https://cna.openjsf.org">cna.openjsf.org</a>	
github.com/fastify/fastify-reply-from/security/advisories/GHSA-gwhp-pf74...	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="https://github.com">github.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	ca

### Vendor Comments And Credit

Discovery Credit

**CNA:** FredKSchott (en)

**CNA:** mcollina (en)

**CNA:** UlisesGascon (en)

**CNA:** climba03003 (en)

There are currently no legacy CID mappings associated with this CVE

There are currently no legacy CID 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 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](#)