



# Fastify request.protocol and request.host spoofable via X-Forwarded-Proto/Host from untrusted connections when trustProxy uses restrictive trust function

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

## Summary

<b>CVE</b>	CVE-2026-3635
<b>State</b>	PUBLISHED
<b>Assigner</b>	openjs
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-23 14:16:34 UTC
<b>Updated</b>	2026-04-16 17:46:58 UTC
<b>Description</b>	Summary When trustProxy is configured with a restrictive trust function (e.g., a specific IP like trustProxy: '10.0.0.1', a subn

## Risk And Classification

**Primary CVSS:** v3.1 6.1 MEDIUM from ce714d77-add3-4f53-aff5-83d477b104bb

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

**Problem Types:** CWE-348 | CWE-348 CWE-348 Use of less trusted source

Version	Source	Type	Score	Severity	Vector
3.1	ce714d77-add3-4f53-aff5-83d477b104bb	Secondary	6.1	MEDIUM	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N
3.1	CNA	CVSS	6.1	MEDIUM	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:N/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 5.8.2 semver	Not specified
CNA	Fastify	Fastify	unaffected 5.8.3 semver	Not specified

### References

Reference	Source	Link	Tags
www.cve.org/CVERecord	ce714d77-add3-4f53-aff5-83d477b104bb	<a href="http://www.cve.org">www.cve.org</a>	Third Party
cna.openjsf.org/security-advisories.html	ce714d77-add3-4f53-aff5-83d477b104bb	<a href="http://cna.openjsf.org">cna.openjsf.org</a>	Third Party
github.com/fastify/fastify/security/advisories/GHSA-444r-cwp2-x5xf	ce714d77-add3-4f53-aff5-83d477b104bb	<a href="https://github.com">github.com</a>	Vendor Ad
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical,

### Vendor Comments And Credit

Discovery Credit

**CNA:** LetaoZhao (TinkAnet) (en)

**CNA:** KaKa (climba03003) (en)

**CNA:** Matteo Collina (en)

**CNA:** Ulises Gascón (en)

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)