@fastify/express vulnerable to middleware authentication bypass via URL normalization gaps (duplicate slashes and semicolons)

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

Summary

CVE	CVE-2026-33808
State	PUBLISHED
Assigner	openjs
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-15 10:16:48 UTC
Updated	2026-04-17 15:38:09 UTC
Description	Impact@fastify/express v4.0.4 and earlier fails to normalize URLs before passing them to Express middleware when Fastify

Risk And Classification

Primary CVSS: v4.0 9.1 CRITICAL from ce714d77-add3-4f53-aff5-83d477b104bb

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/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: 0.001440000 probability, percentile 0.347330000 (date 2026-04-20)

Problem Types: CWE-436 | CWE-436 CWE-436: Interpretation Conflict

Version	Source	Type	Score	Severity	Vector
4.0	ce714d77-add3-4f53-aff5-83d477b104bb	Secondary	9.1	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA
4.0	CNA	CVSS	9.1	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/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	Fastify	@fastify/express	affected 4.0.5 semver	Not specified
CNA	Fastify	@fastify/express	unaffected 4.0.5 semver	Not specified

References

Reference	Source	Link
cna.openjsf.org/security-advisories.html	ce714d77-add3-4f53-aff5-83d477b104bb	cna.openjsf.org
github.com/fastify/fastify-express/security/advisories/GHSA-6hw5-45gm-fj88	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: FredKSchott (en)

CNA: mcollina (en)

CNA: UlisesGascon (en)

CNA: climba03003 (en)

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