



@fastify/express vulnerable to middleware path doubling causing authentication bypass in child plugin scopes

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

Summary

CVE	CVE-2026-33807
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	@fastify/express v4.0.4 and earlier contains a path handling bug in the onRegister function that causes middleware paths to

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from ce714d77-add3-4f53-aff5-83d477b104bb

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

EPSS: 0.000520000 probability, percentile 0.161180000 (date 2026-04-20)

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

Version	Source	Type	Score	Severity	Vector
3.1	ce714d77-add3-4f53-aff5-83d477b104bb	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

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-hrwm-hgmj-7p9c	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.

© 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report