fast-jwt: Empty HMAC secret accepted via async key resolver - JWT auth bypass

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

Summary

CVE	CVE-2026-44351
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 20:16:22 UTC
Updated	2026-05-13 20:16:22 UTC
Description	fast-jwt provides fast JSON Web Token (JWT) implementation. Prior to 6.2.4, a critical authentication-bypass vulnerability ir

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from security-advisories@github.com

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

Problem Types: CWE-287 | CWE-326 | CWE-1391 | CWE-287 CWE-287: Improper Authentication | CWE-326 CWE-326: Inadequate Encryption Strength | CWE-1391 CWE-1391: Use of Weak Credentials

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	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	DECLARED	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

ntegrity

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	Nearform	Fast-jwt	affected < 6.2.4	Not specified

References

Reference	Source	Link	Tags
github.com/nearform/fast-jwt/security/advisories/GHSA-gmvf-9v4p-v8jc	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysi

No vendor comments have been submitted for this CVE.

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