@node-oauth/oauth2-server: PKCE code_verifier ABNF not enforced in token exchange allows brute-force redemption of intercepted authorization codes

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

Summary

CVE	CVE-2026-41213
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-23 19:17:29 UTC
Updated	2026-04-23 19:17:29 UTC
Description	@node-oauth/oauth2-server is a module for implementing an OAuth2 server in Node.js. The token exchange path accepts

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from security-advisories@github.com

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

Problem Types: CWE-307 | CWE-1289 | CWE-307 CWE-307: Improper Restriction of Excessive Authentication Attempts | CWE-1289 CWE-1289: Improper Validation of Unsafe Equivalence in Input

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Node-oauth	Node-oauth2-server	affected < 5.3.0	Not specified

References

Reference	Source	Link	Tags
github.com/node-oauth/node-oauth2-server/security/advisories/GHSA-jhm7-2...	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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