



# @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

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2026-41213  |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | GitHub_M  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2026-04-23 19:17:29 UTC   |
| <b>Updated</b>         | 2026-04-23 19:17:29 UTC   |
| <b>Description</b>     | @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   | <a href="#">CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N</a> |
| 3.1     | CNA                            | DECLARED  | 5.9   | MEDIUM   | <a href="#">CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N</a> |

## 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 | <a href="#">github.com</a>   |           |
| CVE Program record  | CVE.ORG                        | <a href="#">www.cve.org</a>  | canonical |
| NVD vulnerability detail  | NVD                            | <a href="#">nvd.nist.gov</a> | canonical |

No vendor comments have been submitted for this CVE.

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](#) 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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)