

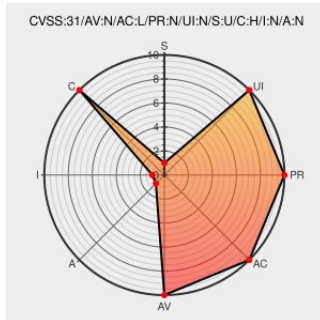


CVE-2017-18924

Published on: 10/04/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:54 PM UTC

CVE-2017-18924

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Oauth2-server](#) from [Oauth2-server Project](#) contain the following vulnerability:

**** DISPUTED **** oauth2-server (aka node-oauth2-server) through 3.1.1 implements OAuth 2.0 without PKCE. It does not prevent authorization code injection. This is similar to CVE-2020-7692. NOTE: the vendor states 'As RFC7636 is an extension, I think the claim in the Readme of "RFC 6749 compliant" is valid and not misleading and I also therefore wouldn't describe this as a "vulnerability" with the library per se.'

CVE-2017-18924 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
RFC 7636 - Proof Key for Code Exchange by OAuth Public Clients	Third Party Advisory tools.ietf.org	MISC tools.ietf.org/html/rfc7636

text/html		
PKCE by visvk · Pull Request #452 · oauthjs/node-oauth2-server · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/oauthjs/node-oauth2-server/pull/452
draft-ietf-oauth-security-topics-15 - OAuth 2.0 Security Best Current Practice	Exploit Third Party Advisory tools.ietf.org text/html	MISC tools.ietf.org/html/draft-ietf-oauth-security-topics-15
Multiple Security Vulnerabilities in Auth and Token Endpoint · Issue #637 · oauthjs/node-oauth2-server · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/oauthjs/node-oauth2-server/issues/637
Missing the Point in Securing OAuth 2.0 by John Tucker codeburst	Third Party Advisory codeburst.io text/html	MISC codeburst.io/missing-the-point-in-securing-oauth-2-0-83968708b467

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[982722](#) Nodejs (npm) Security Update for oauth2-server (GHSA-2fw4-mgq9-39cx)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	OAuth2-server Project	OAuth2-server	All	All	All	All
cpe:2.3:a:oauth2-server_project:oauth2-server:*:*:*:*:node.js:*:*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)