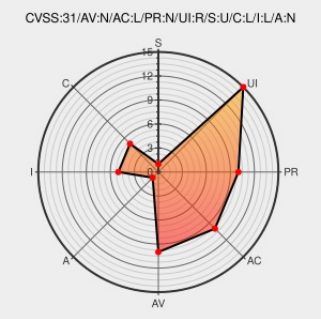
CVE-2023-28848

Published on: Not Yet Published

Last Modified on: 04/10/2023 05:37:00 PM UTC

CVE-2023-28848 - advisory for GHSA-52hv-xw32-wf7f

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of User Oidc from Nextcloud contain the following vulnerability:

user_oidc is the OIDC connect user backend for Nextcloud, an open source collaboration platform. A vulnerability in versions 1.0.0 until 1.3.0 effectively allowed an attacker to bypass the state protection as they could just copy the expected state token from the first request to their second request. Users should upgrade user_oidc to 1.3.0 to receive a patch for the issue. No known workarounds are available.

CVE-2023-28848 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **nextcloud** - **security-advisories** version **= >= 1.0.0, < 1.3.0**

CVSS3 Score: 5.4 - MEDIUM

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

CVE References

Description	Tags	Link
Do not expose the expected code when it does not match by julien-nc · Pull Request #580 · nextcloud/user_oidc · GitHub	github.com text/html	MISC github.com/nextcloud/user_oidc/pull/580
HackerOne	hackerone.com text/html	MISC hackerone.com/reports/1878381
CSRF protection on user_oidc login returned the expected token in case of an error · Advisory · nextcloud/security-advisories · GitHub	github.com text/html	MISC github.com/nextcloud/security-advisories/security/advisories/GHSA-52hv-xw32-wf7f

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nextcloud	User Oidc	All	All	All	All

cpe:2.3:a:nextcloud:user_oidc:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-28848 : user_oidc is the OIDC connect user backend for Nextcloud, an open source collaboration platform. A… twitter.com/i/web/status/1…	2023-04-04 13:06:47
/r/netcve	CVE-2023-28848	2023-04-04 14:38:52

← Previous ID

Next ID→