

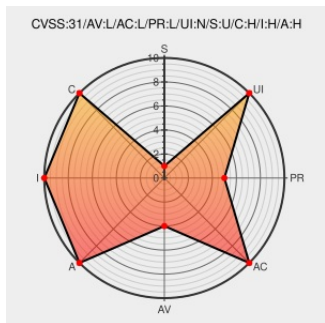


CVE-2023-25820

Published on: Not Yet Published

Last Modified on: 03/29/2023 07:39:00 PM UTC

CVE-2023-25820 - advisory for GHSA-36g6-wjx2-333x

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

Certain versions of [Nextcloud Server](#) from [Nextcloud](#) contain the following vulnerability:

Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, and Nextcloud Enterprise Server is the enterprise version of the file server software. In Nextcloud Server versions 25.0.x prior to 25.0.5 and versions 24.0.x prior to 24.0.10 as well as Nextcloud Enterprise Server versions 25.0.x prior to 25.0.4, 24.0.x prior to

24.0.10, 23.0.x prior to 23.0.12.5, 22.x prior to 22.2.0.10, and 21.x prior to 21.0.9.10, when an attacker gets access to an already logged in user session they can then brute force the password on the confirmation endpoint. Nextcloud Server should upgraded to 24.0.10 or 25.0.4 and Nextcloud Enterprise Server should upgraded to 21.0.9.10, 22.2.10.10, 23.0.12.5, 24.0.10, or 25.0.4 to receive a patch. No known workarounds are available.

CVE-2023-25820 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

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

CVE References

Description	Tags	Link
Missing brute force protection on password confirmation modal - Advisory - nextcloud/security-advisories - GitHub	github.com text/html	MISC github.com/nextcloud/security-advisories/security/advisories/GHSA-36g6-wjx2-333x
HackerOne	hackerone.com text/html	MISC hackerone.com/reports/1842114

Add bruteforce protection to password reset page by pickvergessen - [github.com](#) - [MISC github.com/nextcloud/comm/pull/36480](#)

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	Nextcloud Server	All	All	All	All
Application	Nextcloud	Nextcloud Server	All	All	All	All
cpe:2.3:a:nextcloud:nextcloud_server:*:*:*:*:*:						
cpe:2.3:a:nextcloud:nextcloud_server:*:*:*:enterprise:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-25820 : Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, a... twitter.com/i/web/status/1...	2023-03-22 19:03:12
 @safelabsbr	CVE-2023-25820 Nextcloud Server is the file server software for Nextcloud, a self-hosted pr... twitter.com/i/web/status/1...	2023-03-22 20:55:42
 /r/netcve	CVE-2023-25820	2023-03-22 19:39:35

← Previous ID

Next ID →