



CVE-2023-35172

Published on: Not Yet Published

Last Modified on: 07/05/2023 01:34:00 PM UTC

CVE-2023-35172 - advisory for GHSA-mjf5-p765-qmr6

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N



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

NextCloud Server and NextCloud Enterprise Server provide file storage for Nextcloud, a self-hosted productivity platform. In NextCloud Server versions 25.0.0 until 25.0.7 and 26.0.0 until 26.0.2 and Nextcloud Enterprise Server versions 21.0.0 until 21.0.9.12, 22.0.0 until 22.2.10.12, 23.0.0 until 23.0.12.7, 24.0.0 until 24.0.12.2, 25.0.0 until

25.0.7, and 26.0.0 until 26.0.2, an attacker can bruteforce the password reset links. Nextcloud Server n 25.0.7 and 26.0.2 and Nextcloud Enterprise Server 21.0.9.12, 22.2.10.12, 23.0.12.7, 24.0.12.2, 25.0.7, and 26.0.2 contain a patch for this issue. No known workarounds are available.

CVE-2023-35172 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.1 - CRITICAL**

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

CVE References

Description	Tags	Link
HackerOne	hackerone.com text/html	MISC hackerone.com/reports/1987062
Password reset endpoint is not brute force protected · Advisory · nextcloud/security-advisories · GitHub	github.com text/html	MISC github.com/nextcloud/security-advisories/security/advisories/GHSA-mjf5-p765-qmr6
fix(lostpassword): Also rate limit the setPassword endpoint by	github.com	MISC

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)
 @certbe	Warning: Multiple high-severity vulnerabilities (CVE-2023-35928, CVE-2023-35172, CVE-2023-32320, CVE-2023-32319) in... twitter.com/i/web/status/1...	2023-06-23 14:45:07
 @CVEreport	CVE-2023-35172 : NextCloud Server and NextCloud Enterprise Server provide file storage for Nextcloud, a self-hosted... twitter.com/i/web/status/1...	2023-06-23 21:07:42
 @cracbot	CVE-2023-35172 (CVSS:8.7, HIGH) is Received. NextCloud Server and NextCloud Enterprise Server provide file storage... twitter.com/i/web/status/1...	2023-06-24 06:00:22

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#).

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