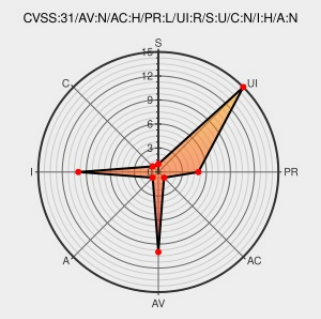
CVE-2021-32733

Published on: 07/12/2021 12:00:00 AM UTC

Last Modified on: 07/14/2021 03:27:00 PM UTC

CVE-2021-32733 - advisory for GHSA-x4w3-jhcr-57pq

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



Certain versions of Nextcloud Server from Nextcloud contain the following vulnerability:

Nextcloud Text is a collaborative document editing application that uses Markdown. A cross-site scripting vulnerability is present in versions prior to 19.0.13, 20.0.11, and 21.0.3. The Nextcloud Text application shipped with Nextcloud server used a `text/html` Content-Type when serving files to users. Due the strict Content-Security-Policy shipped with Nextcloud, this issue is not exploitable on modern browsers supporting Content-Security-Policy. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. As a workaround, use a browser that has support for Content-Security-Policy.

CVE-2021-32733 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **nextcloud** - **security-advisories** version **< 19.0.13**

Affected Vendor/Software: **nextcloud** - **security-advisories** version **>= 20.0.0, < 20.0.11**

Affected Vendor/Software: **nextcloud** - **security-advisories** version **>= 21.0.0, < 21.0.3**

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality	**Integrity**	**Availability**

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
HackerOne	hackerone.com text/html	MISC hackerone.com/reports/1241460
Use text/plain as content type for fetching the document by juliushaertl · Pull Request #1689 · nextcloud/text · GitHub	github.com text/html	MISC github.com/nextcloud/text/pull/1689
XSS in Nextcloud Text application · Advisory · nextcloud/security-advisories · GitHub	github.com text/html	CONFIRM github.com/nextcloud/security-advisories/security/advisories/GHSA-x4w3-jhcr-57pq

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

cpe:2.3:a:nextcloud:nextcloud_server:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-32733 : Nextcloud Text is a collaborative document editing application that uses Markdown. A cross-site sc… twitter.com/i/web/status/1…	2021-07-12 21:11:24
/r/netcve	CVE-2021-32733	2021-07-12 21:41:32

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report