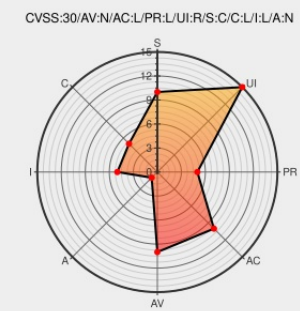
CVE-2018-3780

Published on: 08/13/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:24 PM UTC

CVE-2018-3780

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



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

A missing sanitization of search results for an autocomplete field in NextCloud Server <13.0.5 could lead to a stored XSS requiring user-interaction. The missing sanitization only affected user names, hence malicious search results could only be crafted by authenticated users.

CVE-2018-3780 has been assigned by support@hackerone.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **NextCloud** - **nextcloud/server** version **>13.0.5**

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
advisory – Nextcloud	Vendor Advisory nextcloud.com text/html	CONFIRM nextcloud.com/security/advisory/?id=NC-SA-2018-008

HackerOne	Third Party Advisory hackerone.com text/html	MISC hackerone.com/reports/383117

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:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→