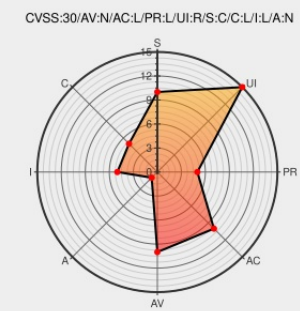
CVE-2018-3781

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

Last Modified on: 03/23/2021 11:24:25 PM UTC

CVE-2018-3781

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



Certain versions of Talk from Nextcloud contain the following vulnerability:

A missing sanitization of search results for an autocomplete field in NextCloud Talk <3.2.5 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-2018-3781 has been assigned by support@hackerone.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **NextCloud** - **nextcloud/talk** version **>=3.2.5**

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-2018-009

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	Talk	All	All	All	All
Application	Nextcloud	Talk	All	All	All	All

cpe:2.3:a:nextcloud:talk:*:*:*:*:*:*:*:*:

cpe:2.3:a:nextcloud:talk:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← 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 registred 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