



CVE-2016-9467

Published on: 03/27/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:17 PM UTC

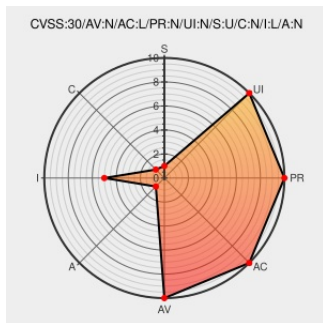
CVE-2016-9467

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

Nextcloud Server before 9.0.54 and 10.0.1 & ownCloud Server before 9.0.6 and 9.1.2 suffer from content spoofing in the files app. The location bar in the files app was not verifying the passed parameters. An attacker could craft an invalid link to a fake directory structure and use this to display an attacker-controlled error message to the user.

CVE-2016-9467 has been assigned by [h](#) support@hackerone.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Filter out %0A from paths · nextcloud/server@778ae8a · GitHub	Issue Tracking Patch Third Party Advisory	MISC github.com/nextcloud/server/commit/778ae8abd54c378fc4781394bbedc7a2ee3095

	github.com text/html	
Also prevent null byte character · nextcloud/server@5dd211c · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	 MISC github.com/nextcloud/server/commit/5dd211cc8845fd4533966bf8d7a7f2a6359ea01
Exclude more invalid chars from files UI path · owncloud/core@e7acbce · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	 MISC github.com/owncloud/core/commit/e7acbce27fa0ef1c6fe216ca67c72d86484919a4
Also prevent null byte character · nextcloud/server@c3ae21f · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	 MISC github.com/nextcloud/server/commit/c3ae21fef2880c9fe44e8fdba1262ac7f9716f14
Exclude more invalid chars from files UI path · owncloud/core@768221f · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	 MISC github.com/owncloud/core/commit/768221fcf3c526c65d85f62b0efa2da5ea00bf2d
#154827 More content spoofing through dir param in the files app - HackerOne	Exploit Third Party Advisory hackerone.com text/html	 MISC hackerone.com/reports/154827
Add PhantomJS to gitignore · nextcloud/server@1352365 · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	 MISC github.com/nextcloud/server/commit/1352365e8bf5ea49da3dc82b1ccf7ddb659ae9
Filter out %0A from paths · nextcloud/server@ed0f0db · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	 MISC github.com/nextcloud/server/commit/ed0f0db5fa0aff04594cb0f973ae4c22b17a175a
advisory – Nextcloud	Patch Vendor Advisory nextcloud.com text/html	 MISC nextcloud.com/security/advisory/?id=nc-sa-2016-010
Security Advisories – ownCloud	Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	 MISC owncloud.org/security/advisory/?id=oc-sa-2016-020
Add PhantomJS to gitignore · nextcloud/server@df50e96 · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	 MISC github.com/nextcloud/server/commit/df50e967dbd27b13875625b7dd3189294619b

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
Application	Owncloud	Owncloud	All	All	All	All
Application	Owncloud	Owncloud	All	All	All	All
cpe:2.3:a:nextcloud:nextcloud_server:*.~.*.*.*.*.*.*.*.						
cpe:2.3:a:nextcloud:nextcloud_server:*.~.*.*.*.*.*.*.*.						
cpe:2.3:a:owncloud:owncloud:*.~.*.*.*.*.*.*.*.						
cpe:2.3:a:owncloud:owncloud:*.~.*.*.*.*.*.*.*.						

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 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