CVE-2016-9460

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-9460
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-28 02:59:00 UTC
Updated	2017-04-04 01:59:00 UTC
Description	Nextcloud Server before 9.0.52 & ownCloud Server before 9.0.4 are vulnerable to a content-spoofing attack in the files app.

Risk And Classification

Problem Types: CWE-284

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nextcloud	Nextcloud	All	All	All	All
Application	Owncloud	Owncloud	All	All	All	All

References

Reference	Source	Link	Tags
Match for /../ · nextcloud/server@8aa0832 · GitHub	MISC	github.com	Issue Tracking, P
HackerOne	MISC	hackerone.com	Exploit, Third Part
Match on 405 · nextcloud/server@dea8e29 · GitHub	MISC	github.com	Issue Tracking, P
Ignore invalid paths in the JS file list (#25368) · owncloud/core@c92c234 · GitHub	MISC	github.com	Issue Tracking, P
Security Advisories – ownCloud	MISC	owncloud.org	Patch, Vendor Ad
Do not allow directory traversal using "../" · nextcloud/server@2da43e3 · GitHub	MISC	github.com	Issue Tracking, P
advisory – Nextcloud	MISC	nextcloud.com	Patch, Vendor Ad
ownCloud and NextCloud CVE-2016-9460 Content Spoofing Vulnerability	BID	www.securityfocus.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysi

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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