



CVE-2022-39211

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-39211
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-16 23:15:00 UTC
Updated	2022-09-21 14:53:00 UTC
Description	Nextcloud server is an open source personal cloud platform. In affected versions it was found that locally running webservice

Risk And Classification

Problem Types: CWE-918

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nextcloud	Nextcloud Enterprise Server	All	All	All	All
Application	Nextcloud	Nextcloud Server	All	All	All	All

References

Reference

- Improve local IP detection by come-nc · Pull Request #33031 · nextcloud/server · GitHub
- Server-Side Request Forgery (SSRF) via potential filter bypass with too lax local domain checking · Advisory · nextcloud/security-advisories · C
- Improve local domain detection by come-nc · Pull Request #32988 · nextcloud/server · GitHub
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)