



# CVE-2021-32656

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

## Summary

<b>CVE</b>	CVE-2021-32656
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-06-01 22:15:00 UTC
<b>Updated</b>	2022-10-25 15:47:00 UTC
<b>Description</b>	Nextcloud Server is a Nextcloud package that handles data storage. A vulnerability in federated share exists in versions pri

## Risk And Classification

**Problem Types:** CWE-284

## NVD Known Affected Configurations (CPE 2.3)

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

## References

Reference	Source	Link
Nextcloud: Multiple Vulnerabilities (GLSA 202208-17) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
Trusted servers exchange can be triggered by attacker · Advisory · nextcloud/security-advisories · GitHub	CONFIRM	<a href="https://github.com">github.com</a>
HackerOne	MISC	<a href="https://hackerone.com">hackerone.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[710590](#) Gentoo Linux Nextcloud Multiple Vulnerabilities (GLSA 202208-17)

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](#)**