



CVE-2021-22906

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

Summary

CVE	CVE-2021-22906
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-11 16:15:00 UTC
Updated	2022-10-25 23:42:00 UTC
Description	Nextcloud End-to-End Encryption before 1.5.3, 1.6.3 and 1.7.1 suffers from a denial of service vulnerability due to permitting

Risk And Classification

Problem Types: CWE-639

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nextcloud	End-to-end Encryption	All	All	All	All

References

Reference	Source	Link
HackerOne	MISC	hackerone.com
End to end encryption folder locking is not properly protected · Advisory · nextcloud/security-advisories · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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