CVE-2021-22879

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

Summary

CVE	CVE-2021-22879
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-14 13:15:00 UTC
Updated	2023-11-07 03:30:00 UTC
Description	Nextcloud Desktop Client prior to 3.1.3 is vulnerable to resource injection by way of missing validation of URLs, allowing a r

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Nextcloud	Desktop	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 33 Update: nextcloud-client-3.1.3-1.fc33 - package-announce - Fedora Mailing-Lists		lists.f
Nextcloud Desktop Client: User-assisted execution of arbitrary code (GLSA 202105-37) — Gentoo security	GENTOO	secu
[SECURITY] Fedora 33 Update: nextcloud-client-3.1.3-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.f
advisory – Nextcloud	MISC	nextc
HackerOne	MISC	hack
Validate sensitive URLs to onle allow http(s) schemes. by allexzander · Pull Request #2906 · nextcloud/desktop · GitHub	MISC	githu
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.r

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

180091 Debian Security Update for nextcloud-desktop (CVE-2021-22879)

281301 Fedora Security Update for nextcloud (FEDORA-2021-1ffffa0251)

710077 Gentoo Linux Nextcloud Desktop Client User-assisted execution of arbitrary code (GLSA 202105-37)

750259 OpenSUSE Security Update for nextcloud-desktop (openSUSE-SU-2021:0577-1)