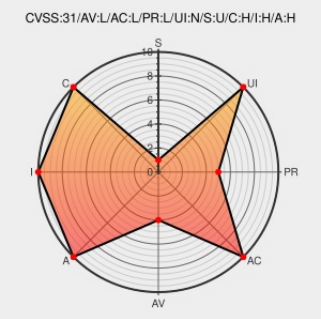
CVE-2020-8224

Published on: 08/10/2020 12:00:00 AM UTC

Last Modified on: 09/30/2022 01:54:00 PM UTC

CVE-2020-8224

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Desktop from Nextcloud contain the following vulnerability:

A code injection in Nextcloud Desktop Client 2.6.4 allowed to load arbitrary code when placing a malicious OpenSSL config into a fixed directory.

CVE-2020-8224 has been assigned by support@hackerone.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
HackerOne	Exploit, Third Party Advisory, hackerone.com, text/html	MISC hackerone.com/reports/622170

Nextcloud Desktop Sync client: Multiple vulnerabilities (GLSA 202009-09) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202009-09
advisory – Nextcloud	Vendor Advisory nextcloud.com text/html	MISC nextcloud.com/security/advisory/?id=NC-SA-2020-030

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:nextcloud:desktop:*:*:*:*:*:*:*:*:

cpe:2.3:a:nextcloud:nextcloud:*:*:*:*:*:windows:*:*:

cpe:2.3:a:nextcloud:nextcloud:*:*:*:*:*:windows:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Openssl - CVE-2020-8224: nextcloud.com/security/advis…	2022-05-24 19:00:38

← Previous ID

Next ID→