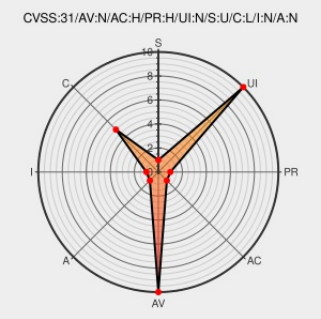
CVE-2020-8173

Published on: 10/30/2020 12:00:00 AM UTC

Last Modified on: 09/27/2022 03:49:00 PM UTC

CVE-2020-8173

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



Certain versions of Nextcloud from Nextcloud contain the following vulnerability:

A too small set of random characters being used for encryption in Nextcloud Server 18.0.4 allowed decryption in shorter time than intended.

CVE-2020-8173 has been assigned by support@hackerone.com to track the vulnerability - currently rated as LOW severity.

CVSS3 Score: 2.2 - LOW

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
HackerOne	Exploit, Third Party Advisory, hackerone.com, text/html	MISC hackerone.com/reports/852841

advisory – Nextcloud	Vendor Advisory nextcloud.com text/html	MISC nextcloud.com/security/advisory/?id=NC-SA-2020-023

There are currently no QIDs associated with this CVE

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i…

Known Affected Configurations (CPE V2.3)

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

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

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

cpe:2.3:a:nextcloud:nextcloud_server:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ? | A too small set of random characters bei... | CVE-2020-8173 | Link for more: alerts.remotelyrmm.com/CVE-2020-8173	2022-09-27 15:29:48

← Previous ID

Next ID→