8

Possibility to force an admin to install recommended applications

Share:

SUMMARY BY NEXTCLOUD

Advisory at https://github.com/nextcloud/security-advisories/security/advisories/GHSA-5vw6-6prg-gvw6

TIMELINE

izorpyan submitted a report to Nextcloud. Nov 17th (about 1 year ago)

Summary:

Endpoint /nextcloud/index.php/core/apps/recommended is accessible via GET http method and doesn't check anti-csrf token. If an admin visits this endpoint in a browser the process of installation of recommended applications begins immediately.

Steps To Reproduce:

1. an attacker creates a malicious page on controlled domain
2. an attacker enforce an admin to visit this page
3. an admin visits this page
4. applications will be installed in a while

Affected version:

nextcloud/server: 22.2.2 (at least)

Recommendation:

require requesttoken for this GET query
or you can change behaviour so to initiate the installation process by manual click (POST query with checking of requesttoken)

[attachment / reference]

Video F1517676: _nextcloud__csrf_install_recommended_app-2021-11-18_00.35.16 4.41 MiB

Zoom in Zoom out Copy Download

0:00 / 2:09

Impact

Increasing of attack surface.
Any unused plugins should be disabled or removed. But this way allows to install them.

1 attachment:
F1517676: _nextcloud__csrf_install_recommended_app-2021-11-18_00.35.16

OT: posted a comment. Nov 17th (about 1 year ago)

Thanks a lot for reporting this potential issue back to us!

Our security team will take a look at this issue as soon as possible. For obvious reasons we'd like to ask you to not disclose this issue to any other party.

nickvergessen Nextcloud staff changed the status to ○ **Triaged**. Nov 18th (about 1 year ago)

Thanks for the report. Seems valid and we will have a look

nickvergessen Nextcloud staff closed the report and changed the status to ○ **Resolved**. Mar 22nd (8 months ago)

Thanks a lot for your report again. This has been resolved in our latest maintenance releases and we're working on the advisories at the moment.

If you have a GitHub account please let us know the username, and we will associate it with the advisory.

igorpyan posted a comment. Mar 22nd (8 months ago)

Hello. Here it is https://github.com/igorpyan. Thank you

Nextcloud rewarded igorpyan with a **$100** bounty. Apr 11th (8 months ago) https://github.com/nextcloud/security-advisories/security/advisories/GHSA-5vw6-6prg-gvw6

Please let us know if you wish any changes to the advisory.

○ nickvergessen Nextcloud staff updated CVE reference to **CVE-2022-24889**. Apr 27th (7 months ago)

○ nickvergessen Nextcloud staff requested to disclose this report. Apr 27th (7 months ago)

igorpyan posted a comment. Apr 29th (7 months ago)

Hi!
Sorry for taking so long. The issue is fixed, I can't reproduce previous behavior. Checked now on 22.2.7.
Thank you.

○ igorpyan agreed to disclose this report. Apr 29th (7 months ago)

○ This report has been disclosed. Apr 29th (7 months ago)