Check the security of your private cloud server

Privacy does not exist without security. To help you keep your data yours, this scan analyzes the security of your server and gives you an overview of what to improve. It only takes into account publicly available information. Therefore it does not reflect on custom patches, support contracts or other particularities of the server in question.

Find out how you can upgrade to Nextcloud to keep your data secure. (https://docs.nextcloud.com/server/latest/go.php?to=admin-update)

Rating

A+

Tweet (https://twitter.com/intent/tweet?
text=I+checked+my+private+cloud+server+with+the+Nextcloud+Security+Scanner+pic.twitter.com%2FfOewONZaAM&via=nextclouders&url=https%3A%2F%2Fscan.nextc

Share (https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fscan.nextcloud.com)

http://mikenextcloud.duckdns.org (http://mikenextcloud.duckdns.org)

Running **Nextcloud 27.1.3.2**

✔ Latest patch level

✔ Major version still supported

Scanned at 2023-11-06 01:58:34   ⟳ trigger re-scan

Vulnerabilities

Learn more about our security efforts. (https://nextcloud.com/secure)

No known vulnerablities.

Hardenings

A security hardening is a feature which protects software from attacks even if it is affected by a certain vulnerability. For an overview of security hardening capabilities we've developed, see our website. (https://nextcloud.com/secure)

Below is a list of hardening features your server has enabled.

✔ Bruteforce protection ⌄

✔ CSPv3 ⌄

✔ Same-Site-Cookies ⌄

✔ Password confirmation ⌄

✔ Checks passwords against HaveIBeenPwned database ⌄

✔ __Host-Prefix ⌄

✔ App passwords can be restricted ⌄

Setup

Besides features of the private cloud software itself, one can configure their Apache or NGINX server more or less securely. Please note that many security settings available cannot be checked from the outside! We strongly recommend you read our Security Hardening Guide (https://docs.nextcloud.com/server/latest/admin_manual/installation/harden_server.html) and follow the instructions there.

Here are the results of a number of checks against your server.

Headers

- ✔ X-Frame-Options ⌄
- ✔ X-Content-Type-Options ⌄
- ✔ X-XSS-Protection ⌄
- ✔ X-Download-Options ⌄
- ✔ X-Permitted-Cross-Domain-Policies ⌄

Our recommendation

We strongly recommend to keep a private cloud server constantly updated. Servers not running the latest security update in a supported release series are often vulnerable. You can find new versions here for Nextcloud (https://nextcloud.com/changelog) and here for ownCloud. (http://owncloud.org/changelog) Nextcloud strives to make upgrading a safe, easy and painless procedure. As a result of these efforts, for users running PHP 7.x and a current version of Nextcloud, there is no need to re-enable apps upon upgrade and users get notified of new versions of apps as well. More improvements are coming! You can learn why and how to upgrade to the latest version of Nextcloud in our earlier blog. (https://nextcloud.com/blog/protect-your-privacy-time-to-upgrade-to-nextcloud-11./)

We further recommend to read our Security Hardening Guide (https://docs.nextcloud.com/server/latest/admin_manual/installation/harden_server.html) and follow the instructions there.

Let us help you keep your data secure

Our customers get proactive help with upgrading and keeping their systems secure. We also warn them in advance when security problems are found. Learn about Nextcloud's security efforts. (https://nextcloud.com/secure)

If you are interested in our services, we have a special time limited offer for prospective customers who can show us a copy of the email warning them of an unsafe instance.

Follow Release News (https://newsletter.nextcloud.com/?p=subscribe&id=4)

Get Expert Help (https://nextcloud.com/enterprise)

Notes

Our scan is strictly based on **publicly available information**, that is the list of known vulnerabilities relevant for ownCloud/Nextcloud releases as well as any applied hardenings/settings we can scan without having access to the server. Find more hardening tips in our hardening guide (https://docs.nextcloud.com/server/latest/admin_manual/installation/harden_server.html) and keep your system up to date.

This is no more than a snapshot in time. Security is an ongoing process and new insights and updates have to be applied to remain secure.

No complicated system can ever be fully secure and even an A+ rated system can be vulnerable to unknown issues and determined (state) attackers.

The rating is automatically generated based on the list of applicable security advisories. The actual risk depends on your environment and may differ.

The rating is calculated as follows:

F = This server version is end of life and has no security fixes anymore. It is likely trivial to break in and steal all the data or even take over the entire server.

E = This server is vulnerable to at least one vulnerability rated "high". It is likely quite easy to break in and steal data or even take over the server.

D = This server is vulnerable to at least one vulnerability rated "medium". With bit of effort, like creating a specially crafted URL and luring a user there, an attacker can likely steal data or even take over the server.

C = This server is vulnerable to at least one vulnerability rated "low". This might or might not provide a way in for an attacker and will likely need some additional vulnerabilities to be exploited.

A = This server has no known vulnerabilities but there are additional hardening capabilities available in newer versions making it harder for an attacker to exploit unknown vulnerabilities to break in.

A+ = This server is up to date, well configured and has industry leading hardening features applied, making it harder for an attacker to exploit unknown vulnerabilities to break in. Learn more about these preventive hardening features. (https://nextcloud.com/blog/nextcloud-11-delivers-verified-security-improvements)

Disclaimer

This security check is for Nextcloud cloud servers only. Nextcloud can not guarantee exact and/or proper results with other cloud servers than Nextcloud.

© 2021 Nextcloud, Legal Notice (https://nextcloud.com/impressum/) and Privacy policy (https://nextcloud.com/privacy)