16

Reflected XSS when renaming a file with a vulnerable name which results in an error

Share:

TIMELINE

yzy9951 submitted a report to **Nextcloud**. Jun 12th (3 years ago)

Hi,

It looks like Nextcloud team will accept the XSS protected by the CSP. (Report #896511)
Here is another XSS.

1. Rename an existing filename to `<img src=x onerror=prompt(1)>` .jpg.
2. Anyone tries to rename this `<img src=x onerror=prompt(1)>` .jpg with an invalid filename, like add a "\" in it, will trigger the XSS attack.
3. Need bypass the CSP.

Thanks

Impact

Cross-Site Scripting

2 attachments:
F865153: XSS.png
F865154: Add_PoC.png

BOT: posted a comment. Jun 12th (3 years 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. We will reply to your report within 72 hours, usually much faster. For obvious reasons we'd like to ask you to not disclose this issue to any other party.

nickvergessen Nextcloud staff posted a comment. Jun 12th (3 years ago)

Thanks for your report again, I forwarded it to the correct developers

nickvergessen Nextcloud staff changed the status to ○ **Triaged**. Jun 12th (3 years ago)

nickvergessen Nextcloud staff posted a comment. Jan 20th (2 years ago)

Pull request at https://github.com/nextcloud/server/pull/25234

Nextcloud rewarded yzy9951 with a **$100** bounty. Jan 20th (2 years ago)

Congratulations! We have determined this to be eligible for a reward of $100.

Thanks a lot for making the internet a safer place and keep hacking. Please keep in mind that we didn't patch the vulnerability yet, so please do not share this information with any third-parties.

nickvergessen Nextcloud staff closed the report and changed the status to ○ **Resolved**. Feb 2nd (2 years 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.

Please let us know how you'd like to be credited in our official advisory. We require the following information:

- Name / Pseudonym
- Email address (optional)
- Website (optional)
- Company (optional)

yzy9951 posted a comment. Feb 2nd (2 years ago)

Hi @nickvergessen,

Name: Zhouyuan Yang
Website: https://www.fortiguard.com/
Company: Fortinet

By the way, can you request a CVE ID for it, please?

Thanks!

nickvergessen Nextcloud staff changed the report title from **XSS in rename** to **Reflected XSS when renaming a file with a vulnerable name which results in an error**. Feb 10th (2 years ago)

nickvergessen Nextcloud staff posted a comment. Feb 10th (2 years ago)

Pending SA: https://nextcloud.com/security/advisory/?id=NC-SA-2021-00
Pending CVE: CVE-2021-22878

Scheduled date: 22nd feb (4weeks after 20.0.6 release)

nickvergessen Nextcloud staff requested to disclose this report. Mar 1st (2 years ago)