


20 XSS through image upload of contacts using svg file with png extension

Share:     


TIMELINE

 bitman_47 submitted a report to [Nextcloud](#). Oct 5th (2 years ago)
Hello again, this is a bypass [#89487](#) basically use the same payload file but change the extension to PNG

Impact


XSS or Open redirect when viewing the image of a contact

1 attachment:
[F1015209: redirectxss.svg.png](#)

 brthnc posted a comment. Oct 5th (2 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.

 bitman_47 posted a comment. Oct 5th (2 years ago)
Sorry I meant a bypass of [#894876](#)

 brthnc [Nextcloud staff](#) posted a comment. Oct 12th (2 years ago)
Hey!
I cannot reproduce this. The viewer displays an error because it can't display the file.
Could you elaborate on a step-by-step process on how you get it to be displayed?

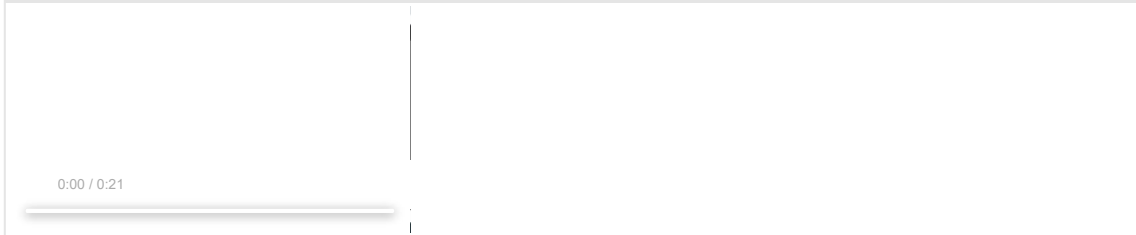
 brthnc [Nextcloud staff](#) changed the status to [Needs more info](#). Oct 12th (2 years ago)

 bitman_47 changed the status to [New](#). Updated Oct 12th (2 years ago)
Sorry, I should have provided all the steps,

1. Use Chrome/Chromium as it does not work in Firefox
2. Upload the "image"
3. Click on the small image so it pops up as modal
4. Open image in new tab


Video F1032532: recording-1602503965782.webm 2.05 MiB



[Zoom in](#) [Zoom out](#) [Copy](#) [Download](#)




1 attachment:
[F1032532: recording-1602503965782.webm](#)

 brthnc [Nextcloud staff](#) posted a comment. Oct 12th (2 years ago)
Ah right, still in contacts!
I thought you meant in files :)
Thanks!

 bitman_47 posted a comment. Oct 12th (2 years ago)
No problem. In files it still works without the png extension, I thought maybe you guys decided it was acceptable behavior in there.

 bitman_47 posted a comment. Oct 16th (2 years ago)
 brthnc, I think you forgot to triage this report and Would you like me to submit a separate report for files?

 bitman_47 posted a comment. Oct 27th (2 years ago)
I saw this was resolved, good job on the new implementation.

 nickvergessen [Nextcloud staff](#) closed the report and changed the status to [Resolved](#). Oct 28th (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.

- Email address (optional)
- Website (optional)
- Company (optional)



hitman_47 posted a comment.

I can be credited as Tommy Suriel. Thank you for always working well with me.

Oct 28th (2 years ago)



nickvergessen Nextcloud staff posted a comment.

Always a pleasure to work with your reports instead of the spammy non-responsive or nasty bugging reporters.

Btw did you receive a Nextcloud Swag/TShirt yet? Otherwise I will award you with one (additionally) finally.

Oct 28th (2 years ago)



hitman_47 posted a comment.

Thank you, I have not received a swag, that would be nice. Thanks.

Oct 28th (2 years ago)



nextcloud has decided that this report is not eligible for a bounty.

The contacts app is not eligible for bounties

Nov 17th (2 years ago)



nickvergessen Nextcloud staff posted a comment.

CVE pending: [CVE-2020-8280](#)

Advisory will be published at <https://nextcloud.com/security/advisory/?id=NC-SA-2020-044>

Nov 17th (2 years ago)



hitman_47 posted a comment.

Thanks for the update

Nov 17th (2 years ago)



nickvergessen Nextcloud staff requested to disclose this report.

Nov 26th (2 years ago)



This report has been disclosed.

Dec 26th (2 years ago)