


## 18 XSS through image upload of contacts using svg file

Share:     

### TIMELINE

- 


hitman\_47 submitted a report to Nextcloud. This is a bypass of report #808287

Jun 9th (3 ye
- Upload the attached file for the image of a contact, right click "Open image in new tab" and you will see the xss.

**Impact**

The person viewing the image of a contact can be victim of XSS.


1 attachment:

F861335: redirect.svg
- 

OT: posted a comment.


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.

Jun 9th (3 ye
- 

hitman\_47 posted a comment.


FYI, this can also work as an open redirect by changing the value of onload in the svg file to "window.location='http://www.example.com'".

Jun 10th (3 ye
- 


nickvergessen (Nextcloud staff) posted a comment.

More accurate 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


Jun 12th (3 ye
- 

nickvergessen (Nextcloud staff) changed the status to Triaged.

Jun 12th (3 ye
- 


hitman\_47 posted a comment.

Correct, thanks! Sorry for the missing steps.

Jun 12th (3 ye
- 

hitman\_47 posted a comment.


I also noticed this works on the general file upload endpoint nextcloud.com/apps/files. Same steps and conditions.

Jun 19th (2 ye
- 

hitman\_47 posted a comment.


To be clear:

  1. Go to nextcloud.com/apps/files using chrome or chromium
  2. Upload the same svg file.
  3. Click it and once it opens in the modal, open the image in a new tab.

Jun 19th (2 ye
- 


hitman\_47 posted a comment.

Hello, any updates on this?

Sep 2nd (2 ye
- 


brthnc (Nextcloud staff) posted a comment.

Hi @hitman\_47 a fix was dispatched, but it create a usability issue. We're fixing it.

Sep 5th (2 ye
- 


hitman\_47 posted a comment.

Great, thanks for the update

Sep 5th (2 ye
- 

brthnc (Nextcloud staff) posted a comment.


All fixes have been merged. This is waiting for release.

Sep 7th (2 ye
- 

nickvergessen (Nextcloud staff) closed the report and changed the status to Resolved.









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

Sep 7th (2 ye
- 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)
- 

hitman\_47 posted a comment.

Sep 7th (2 ye

 <b>brthnc</b> <small>Nextcloud staff</small> posted a comment. Did you test master?	Sep 7th (2 ye
 <b>hitman_47</b> posted a comment. Oh no sorry , I just tested the online demo	Sep 7th (2 ye
 <b>brthnc</b> <small>Nextcloud staff</small> posted a comment. All good! We'll release the new contacts in the upcoming weeks :)	Sep 7th (2 ye
 <b>nickvergessen</b> <small>Nextcloud staff</small> posted a comment. CVE pending: <a href="#">CVE-2020-8281</a> Advisory will be published at <a href="https://nextcloud.com/security/advisory/?id=NC-SA-2020-045">https://nextcloud.com/security/advisory/?id=NC-SA-2020-045</a>	Nov 17th (2 ye
 <b>nextcloud</b> rewarded <b>hitman_47</b> with a \$100 bonus. The contacts app is not eligible for bounties, but we agreed on giving you a bonus for all the digging around the contacts app.	Nov 17th (2 ye
 <b>nickvergessen</b> <small>Nextcloud staff</small> requested to disclose this report.	Nov 17th (2 ye
 <b>hitman_47</b> posted a comment. Thank you!	Nov 17th (2 ye
 This report has been disclosed.	Dec 17th (2 ye