

23

## Bypass of privacy filter / tracking pixel blocker

Share:     

## TIMELINE



Foobar7 submitted a report to Nextcloud.

Jun 2nd (2 years ago)

## Description

When the mail app receives inline images, it will block them for privacy reasons to prevent tracking pixels ( `The images have been blocked to protect your privacy` ).

This block works correctly for most remote resources (in addition to images, remote CSS files, iframes, and some CSS attributes are also blocked).

However, it is still possible to inject images via some CSS attributes (specifically, `list-style-image` and `background-image` ), thus bypassing the block and enabling tracking of users.

## POC

Send a mail with the following body to an email address that is connected to Nextcloud Mail (the HTML code can for example be sent via thunderbird by clicking insert - > HTML):

Code 408 Bytes [Wrap lines](#) [Copy](#) [Download](#)

```
1 <style>
2     big {
3         background-image: url(https://www.google.com/logos/doodles/2021/celebrating-frank-kameny-6753651837108392-1.png);
4     }
5 }
6 ul {
7     list-style-image: url(https://www.google.com/logos/doodles/2021/celebrating-frank-kameny-6753651837108392-1.png);
8 }
9 </style>
10 <big>test</big>
11
12 <ul>
13     <li>Item 1</li>
14     <li>Item 2</li>
15 </ul>
```

Open the message to see that the remote image is included directly, bypassing the privacy filter. An attacker can now replace `www.google.com` with a log server they control to log when users open the mail.

## Impact

bypass of image privacy filter which prevents tracking scripts from gathering users IP addresses and information on when they view an email.



OT: posted a comment.

Jun 2nd (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.

lukasreschenc changed the status to Triaged.

Jun 2nd (2 years ago)

Thanks for the report, I was able to reproduce the fact that images are displayed without user-interaction.

However, it seems that the images are still proxied via the Nextcloud instance. So it doesn't seem like there is an IP address leakage. If you manage to trigger a direct connection, please do let us know as this increases the severity a bit.



Foobar7 posted a comment.

Jun 2nd (2 years ago)

Hi @lukasreschenc,

thanks for looking into this! You are right, that was my mistake. I double-checked, and all images are correctly proxied. The issue can still be used to track individual users, but it will not reveal their IP.

Best,  
Foobar7



lukasreschenc posted a comment.

Jun 16th (2 years ago)

The product team is working for a patch for this at <https://github.com/nextcloud/mail/pull/5189>



lukasreschenc posted a comment.

Jun 23rd (about 1 year ago)

Draft advisory is at <https://github.com/nextcloud/security-advisories/security/advisories/GHSA-xxp4-44xc-8crh>

lukasreschenc updated CVE reference to [CVE-2021-32707](#).


Jun 23rd (about 1 year ago)



Nextcloud rewarded foobar7 with a \$100 bounty.

Jun 23rd (about 1 year ago)

Congratulations! We have determined this to be eligible for a reward of \$100. As there was no IP leakage and the risk was thus minimal.




lukasreschke

closed the report and changed the status to **resolved**.

Jun 25th (about 1 year ago)


Thanks a lot for your report again. This will be resolved in our next maintenance releases, likely scheduled for early July. Please do not disclose any details about this earlier. (feel free to request disclosure on HackerOne here, the 30 day countdown should be sufficient :))

We have also associated your GitHub account with above advisory, and will publish it 1-2 weeks after the release.



lukasreschke requested to disclose this report.

Jul 12th (about 1 year ago)



This report has been disclosed.

Aug 11th (about 1 year ago)