16 XSS in desktop client via invalid server address on login form

Share:

TIMELINE

jplopezy submitted a report to Nextcloud. Aug 31st (3 years ago)

Team!

I have found this vulnerability that in my time would be called "cross zone" but at the moment I don't know.

The problem is found in the latest version of "nextcloud.exe" for your windows version.

The problem occurs with the initial screen where you ask to connect to a website.

Apparently when you put an invalid URI that generates some type of response code like 403, it is reported in a small window, as if it were an alert box, not in the main.

This "alert box" visualizes the response and to my impression (that's why I said the cross zone) has a little more permissions than the internet explorer.

For example, if the response code has an `<S>` test `</S>` it will interpret it as IE does.

That's fine, it would only be an html injection.

The problem, for example, is that it allows you to run a file like the calculator locally without any confirmation.

This vector works : `<A HREF="file:///C:/WINDOWS/system32/calc.exe">` CALC.EXE `</A>`

In my opinion, response code errors are a problem and must be controlled by the application.

For the demonstration use the burp.

But basically any personal site where the response code building could be controlled could exploit it.

I attach a video to make everything clearer.

Impact

The impact is that you can run local files without authorization (of the application) in a context where you should warn.

It should be filtered so as not to disturb that it is a vector.

1 attachment:
F571293: nextcloud.webm

OT: posted a comment. Aug 31st (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.

ullzer posted a comment. Sep 3rd (3 years ago)

Hi @jplopezy,

Thanks for your report.
We are working with our desktop team to look into this.

We'll keep you posted.

Cheers,
--Roeland

nickvergessen Nextcloud staff changed the status to ○ Triaged. Sep 5th (3 years ago)

jplopezy posted a comment. Nov 4th (3 years ago)

I hope you are well! something new ?

ullzer posted a comment. Mar 21st (3 years ago)

Hi @jplopezy

So we had some discussion how to fix this. The issue is that in some cases it could have useful information.
However we decided that it is probably better to just remove the message box.

The PR to do this is in https://github.com/nextcloud/desktop/pull/1885

Cheers,
--Roeland

ickvergessen Nextcloud staff closed the report and changed the status to ○ Resolved. Jun 9th (3 years ago)

Thanks a lot for your report again. This has been resolved for our next 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:

jplopezy posted a comment. Jun 9th (3 years ago)

Name / Pseudonym : Juan Pablo Lopez Yacubian

nickvergessen Nextcloud staff updated the severity to Medium (4.7). Jun 25th (2 years ago)

nickvergessen Nextcloud staff changed the report title from **Uncontrolled Response Code Html Injection** to **XSS in desktop client via invalid server address on login form**. Jun 25th (2 years ago)

nickvergessen Nextcloud staff posted a comment. Jun 25th (2 years ago)

SA will be published at https://nextcloud.com/security/advisory/?id=NC-SA-2020-027
Requested CVE: CVE-2020-8189

Nextcloud rewarded jplopezy with a **$100** bounty. Jun 25th (2 years ago)

nickvergessen Nextcloud staff requested to disclose this report. Aug 5th (2 years ago)

jplopezy agreed to disclose this report. Aug 16th (2 years ago)

This report has been disclosed. Aug 16th (2 years ago)