6

Malicious apps can crash Nextcloud Android client by sending malformed intents

Share:

TIMELINE

bigbug submitted a report to Nextcloud. Apr 25th (3 years ago)

Not sure if this can be tracked as a security issue, but this definitely calls for a code change. This can be classified into Denial of Service category attack and can seriously hamper user experience.

Asset: Nexcloud Android Client (com.nextcloud.client)
Version: 3.11.1 (latest)

Details

The Nextcloud android app registers a deeplink `nc://login` that is handled by the `com.owncloud.android.authentication.ModifiedAuthenticatorActivity` class as seen in AndroidManifest file.

The above mentioned class implements `AuthenticatorActivity` class in order to handle incoming deeplinks.

It is seen that the method `parseLoginDataUrl` does not handle exception correctly crashing the Nextcloud app.

malicious apps can thus crash the nextcloud client by sending following data in intent : `nc://login`.

ADB payload:

Code 195 Bytes Wrap lines Copy Download

```
adb shell am start -a "android.intent.action.VIEW" -c "android.intent.category.DEFAULT" -n "com.nextcloud.client/com.owncloud.android.authentication.Modifie
```

Attaching video PoC

Video F803256: nextcloud_intent_crash.mp4 1.34 MiB

Zoom in Zoom out Copy Download

0:00 / 0:25

Impact

1. Malicious apps can crash the nextcloud android client to cause a denial of service attack.

1 attachment:
F803256: nextcloud_intent_crash.mp4

BOT: posted a comment. Apr 25th (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.

nickvergessen Nextcloud staff posted a comment. Apr 27th (3 years ago)

Ad per our threat model https://nextcloud.com/security/threat-model/ such attacks are not high risk, but I notified the android developers to check if it is possible to at least not crash.

> Attacks involving other Android apps on the device
>
> We do consider attacks involving other Android apps on the device as low or medium risk. Stored files can be hidden from other apps if appropriate storage option is selected inside the app. This should be secure, however, if the phone is compromised we don't guarantee data safety.

bigbug posted a comment. Apr 28th (3 years ago)

Hi @nickvergessen - Thanks for looking into this. Can you provide if/how this report will be tracked further?

nickvergessen Nextcloud staff changed the status to ○ Triaged. May 4th (3 years ago)

Thanks again for your report. We currently don't see this as a high risk, so it will be resolved at a later time.

bigbug posted a comment. May 19th (3 years ago)

Hi @nickvergessen - Could you address the reports now?

bigbug posted a comment. Jan 31st (2 years ago)

Apologies for the delay here. We'll follow-up with the engineering team on the state.

bigbug posted a comment. Feb 1st (2 years ago)

Thanks for update @lukasreschkenc.
Request you to also look at https://hackerone.com/reports/859575.

tobiaskaminsky Nextcloud staff posted a comment. Feb 2nd (2 years ago)

Fix is at: https://github.com/nextcloud/android/pull/7919

bigbug posted a comment. Feb 5th (2 years ago)

Hi @lukasreschkenc and @tobiaskaminsky - also have a look at https://hackerone.com/reports/859575. This was also submitted along with this report and has much higher impact.

nickvergessen Nextcloud staff closed the report and changed the status to ○ Resolved. Feb 12th (2 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)

bigbug posted a comment. Feb 12th (2 years ago)

Hi @nickvergessen - Thanks. Please find below my name to be published:

Name: Sarath Sasikumar

bigbug posted a comment. Feb 15th (2 years ago)

@nickvergessen - Is this eligible for reward?

lukasreschkenc posted a comment. Feb 16th (2 years ago)

Our bounty panel is in the progress of discussing the bounties for this issue. We'll update you once we have come to a conclusion.

bigbug posted a comment. Feb 23rd (2 years ago)

@lukasreschkenc - Is the advisory published? Also which version of the app in play store contains the patch for this issue?

bigbug posted a comment. Feb 28th (2 years ago)

Hi @lukasreschkenc - Any updates?

lukasreschkenc posted a comment. Mar 1st (2 years ago)

As per our Android team the release which will fix this vulnerability will be 3.15.1 and is planned to be released this week.

We usually publish advisories 2 weeks after the release of the patch.

Nextcloud has decided that this report is not eligible for a bounty. Mar 1st (2 years ago)

As per our current program policy, we are not awarding monetary rewards for Denial of Service issues:

> At the moment we are also considering Denial of Service not a reward worthy vulnerability. (we will acknowledge you though!)

We'll be working on the advisories and let you know once we have them.

bigbug posted a comment. Apr 6th (2 years ago)

Hi @lukasreschkenc - Let me know if the advisory is published. Thanks

bigbug posted a comment. Apr 17th (2 years ago)

@lukasreschkenc - could you please point me to the published advisory?

bigbug posted a comment. Jun 15th (2 years ago)

@lukasreschkenc - Is the advisory published yet? Kindly update.

lukasreschkenc posted a comment. Jun 16th (2 years ago)

Apologies. We moved to a new advisory platform and as this has not been marked as eligible for a bounty, we missed it.

The advisory will be at https://github.com/nextcloud/security-advisories/security/advisories/GHSA-h2gm-m374-99vc and is pending CVE assignment. If you let us know your GitHub handle we can associate your account with the advisory.

bigbug posted a comment. Jun 16th (2 years ago)

@lukasreschkenc - Thanks for your response.

My GitHub handle is R0b0t4ng3nt

lukasreschkenc updated CVE reference to CVE-2021-32694. Jun 17th (about 1 year ago)

lukasreschkenc requested to disclose this report. Jun 17th (about 1 year ago)

Thank you @lukasreschkenc. Disclosing the report.

This report has been disclosed.

Jun 17th (about 1 year ago)