\equiv



TIMELINE

daniel_calvino_sanchez submitted a report to Nextcloud.

May 28th (3 years ago)

- Create a new mail share with a password by using the OCS endpoint with something like: $curl-u\ admin: admin: admin-X\ POST-H\ "OCS-APIR equest: true"\ "http://localhost/ocs/v1.php/apps/files_sharing/api/v1/shares?$ path=welcome.txt&shareType=4&shareWith=user@server.com&password=plainTextPassword"
- $\bullet \quad \text{Check the last item in the "oc_share" table in the database; the stored password is "plainTextPassword" instead of a hashed version.}\\$

Note that the password is properly hashed if the password is autogenerated

 $(https://github.com/nextcloud/server/blob/caff1023ea72bb2ea94130e18a2a6e2ccf819e5f/apps/sharebymail/lib/ShareByMailProvider.php\#L236) \ or if the share is the$ later updated with another password

(https://github.com/nextcloud/server/blob/16da29caba1cefa4c0762fae6014d6d2c737ee94/lib/private/Share20/Manager.php#L1085).

Impact

An attacker would be able to get the plain text password of a mail share.

OT: posted a comment. hanks a lot for reporting this potential issue back to us!

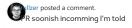
May 28th (3 years ago)

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 to ask the factor of tyou to not disclose this issue to any other party.

O-rullzer changed the status to o Triaged.

extcloud has decided that this report is not eligible for a bounty. nternal report

May 28th (3 years ago)



May 28th (3 years ago)

ickvergessen Nextcloud staff closed the report and changed the status to • Resolved.

Jun 8th (3 years ago)

Pickvergessen (Nextdood staff) closed the report and changed the status to γ nessores.

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)

O- nickvergessen Nextcloud staff requested to disclose this report.

Sep 28th (2 years ago)

O- This report has been disclosed.

Oct 28th (2 years ago)