4

Error in Deleting Deck cards attachment reveals the full path of the website

Share:

SUMMARY BY NEXTCLOUD

Advisory at https://github.com/nextcloud/security-advisories/security/advisories/GHSA-hx9w-xfrg-2qvp

TIMELINE

ctulhu submitted a report to Nextcloud. Sep 29th (about 1 year ago)

Summary:

An error in deck cards when deleting an attachment reveals the full path of the website.

Code 503 Bytes Wrap lines Copy Download

```
DELETE /apps/deck/cards/11/attachment/file:1 HTTP/2
Host: ctulhu.me/nc
Sec-Ch-Ua: "Chromium";v="93", " Not;A Brand";v="99"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Sec-Ch-Ua-Platform: "macOS"
Origin: https://ctulhu.me/nc
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Response

Code 2.81 KiB Wrap lines Copy Download

```
Content-Length: 2057
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-Control: no-cache, no-store, must-revalidate
Content-Security-Policy: default-src 'none';base-uri 'none';manifest-src 'self';frame
Feature-Policy: autoplay 'none';camera 'none';fullscreen 'none';geolocation 'none';mi
X-Robots-Tag: none
Referrer-Policy: no-referrer
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Frame-Options: SAMEORIGIN
X-Permitted-Cross-Domain-Policies: none
X-Robots-Tag: none
X-Xss-Protection: 1; mode=block
Cf-Cache-Status: DYNAMIC
Server: cloudflare
Cf-Ray: 69639391d9741f21-FRA
Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=

{"status":500,"message":"There was an error retrieving the share. Maybe the link is
```

Steps To Reproduce:

[add details for how we can reproduce the issue]

- 0.) setup burpsuite
- 1.) go to $website/apps/deck and pick any cards
- 2.) attach a file to the card and delete it
- 3.) On burp suite go to proxy > http history > find the request
- 4.) send the request to repeater and run the request again

Impact

Full path disclosure

OT: posted a comment. Sep 29th (about 1 year ago)

Thanks a lot for reporting this potential issue back to us!

lukasreschkenc changed the status to ○ **Needs more info**. Oct 4th (about 1 year ago)

Thanks for your report, much appreciated.

Could you verify that you haven't enabled `debug` in your `config.php`? From reading the code, it seems to me that the exception message should only appear in debug mode.

ctulhu changed the status to ○ **New**. Oct 4th (about 1 year ago)

Hi! This was tested on our staging server which is uses the same config in our production server. So `debug` is not enabled in `config.php`, Would you like me to send you a copy of our config.php?

Code 701 Bytes Wrap lines Copy Download

```
root@server:/var/www/html/config# grep -r "debug" *
config.sample.php: * Enable SMTP class debugging.
config.sample.php:'mail_smtpdebug' => false,
config.sample.php: * conditions is met, the required log level is set to debug. This
config.sample.php: * debug specific requests, users or apps
config.sample.php: * debugging, as your logfile will become huge.
config.sample.php: * Enable locking debug logging
config.sample.php:'filelocking.debug' => false,
config.sample.php: * Set this Nextcloud instance to debugging mode
config.sample.php: * This will disable the minifier and outputs some additional debu
config.sample.php:'debug' => false,
root@server:/var/www/html/config#
```

lukasreschkenc changed the status to ○ **Needs more info**. Oct 4th (about 1 year ago)

I have some trouble reproducing the issue, in my testing it never returns any exception details:

Code 128 Bytes Wrap lines Copy Download

```
{"status":500,"message":"There was an error retrieving the share. Maybe the link is w
```

Would you be able to run the following command and share the return value with us?

Code 43 Bytes Wrap lines Copy Download ctulhu changed the status to ○ New.

Updated Mar 9th (9 months ago)

`sudo -u www-data php occ config:list system`

Output

Code 2.36 KiB   Wrap lines Copy Download

```
{
    "system": {
        "memcache.local": "\\OC\\Memcache\\APCu",
        "apps_paths": [
            {
                "path": "\/var\/www\/[redacted]\/apps",
                "url": "\/apps",
                "writable": false
            },
            {
                "path": "\/var\/www\/[redacted]\/custom_apps",
                "url": "\/custom_apps",
                "writable": true
            }
        ],
        "instanceid": "***REMOVED SENSITIVE VALUE***",
        "passwordsalt": "***REMOVED SENSITIVE VALUE***",
        "secret": "***REMOVED SENSITIVE VALUE***",
        "trusted_domains": [
            "[redacted]"
        ],
        "datadirectory": "***REMOVED SENSITIVE VALUE***",
        "dbtype": "mysql",
        "version": "22.1.1.2",
        "overwrite.cli.url": "https:\/\/[redacted]",
        "dbname": "***REMOVED SENSITIVE VALUE***",
        "dbhost": "***REMOVED SENSITIVE VALUE***",
        "dbport": "1337",
        "dbtableprefix": "oc_",
        "mysql.utf8mb4": true,
        "dbuser": "***REMOVED SENSITIVE VALUE***",
            "class": "OC\\Files\\ObjectStore\\S3",
            "arguments": {
                "bucket": "[redacted]",
                "key": "***REMOVED SENSITIVE VALUE***",
                "secret": "***REMOVED SENSITIVE VALUE***",
                "use_ssl": true,
                "use_path_style": true,
                "region": "[redacted]"
            }
        },
        "mail_smtpmode": "smtp",
        "mail_smtpauth": 1,
        "mail_sendmailmode": "smtp",
        "mail_smtpauthtype": "LOGIN",
        "mail_smtpsecure": "ssl",
        "mail_from_address": "***REMOVED SENSITIVE VALUE***",
        "mail_domain": "***REMOVED SENSITIVE VALUE***",
        "mail_smtpname": "***REMOVED SENSITIVE VALUE***",
        "mail_smtppassword": "***REMOVED SENSITIVE VALUE***",
        "mail_smtphost": "***REMOVED SENSITIVE VALUE***",
        "mail_smtpport": "465",
        "force_language": "en",
        "twofactor_enforced": "false",
        "twofactor_enforced_groups": [
            "Administrative"
        ],
        "twofactor_enforced_excluded_groups": [],
        "overwritehost": "[redacted]",
        "overwriteprotocol": "https",
        "updater.secret": "***REMOVED SENSITIVE VALUE***",
        "maintenance": false,
        "theme": "",
        "loglevel": 2
    }
}
```

ctulhu posted a comment. Oct 5th (about 1 year ago)

Code 128 Bytes Wrap lines Copy Download

```
{"status":500,"message":"There was an error retrieving the share. Maybe the link is w
```

lukasreschkenc posted a comment. Oct 19th (about 1 year ago)

The controller code that is invoked can be seen at https://github.com/nextcloud/deck/blob/6caa7bcfcbbfb618a546f824f67851c3f4fee9e5/lib/Service/AttachmentService.php#L327-L363.

Based on your stack trace, the issue seems to be within "extendData", which can be found at https://github.com/nextcloud/deck/blob/6caa7bcfcbbfb618a546f824f67851c3f4fee9e5/lib/Service/FilesAppService.php#L138-L157

The relevant code here is:

Code 66 Bytes Wrap lines Copy Download

```
$share = $this->shareProvider->getShareById($attachment->getId());
```

Which calls into https://github.com/nextcloud/deck/blob/6caa7bcfcbbfb618a546f824f67851c3f4fee9e5/lib/Sharing/DeckShareProvider.php#L567-L600, and throws a `ShareNotFound` exception at line 586.

When I changed this to throw an exception manually this indeed showed an exception trace.

Thanks for your patience, I have filed a ticket for the product team and we'll let you know one we received an update.

lukasreschkenc changed the status to ○ **Triaged**. Oct 19th (about 1 year ago)

ctulhu posted a comment. Oct 19th (about 1 year ago)

Hi @lukasreschkenc, Can you also take a look at #1338781 ? Still no bounty yet.
In a few days the report will reach its 30th day since it was resolved.

lukasreschkenc posted a comment. Oct 25th (about 1 year ago)

Apologies for the delay here. We have issued a bounty for this report now.

≡

ctulhu posted a comment. Dec 2nd (12 months ago)

Hi! @lukasreschkenc, I hope you are doing well. Seems like the new version was released two days ago, Do we have any new updates?

thanks!

ctulhu has requested mediation from HackerOne Support. Jan 6th (11 months ago)

The fix has been released last month and there are still no updates.

nickvergessen Nextcloud staff closed the report and changed the status to ○ **Resolved**. Jan 7th (11 months ago)

Thanks a lot for your report again. This has been resolved in a maintenance releases and we're working on the advisories at the moment.

If you have a GitHub account please let us know the username, and we will associate it with the advisory.

nickvergessen Nextcloud staff posted a comment. Jan 7th (11 months ago)

Hi, sorry for the delay. Lukas is taking a break currently and it seems the forwarding of tasks didn't work as planned.

ctulhu posted a comment. Jan 7th (11 months ago)

Hi @nickvergessen!

No worries, Will also be the issuing of bounty delayed?

nickvergessen Nextcloud staff posted a comment. Jan 10th (11 months ago)

Yes, but you should get a response soon

ctulhu posted a comment. Jan 28th (10 months ago)

Hi @nickvergessen It has been 18 days. Do we have new updates on the bounty?

thanks.

nickvergessen Nextcloud staff posted a comment. Feb 7th (10 months ago)

I suggested an amount now and will ask for another person to approve the bounty. Sorry for taking so long.

Hi! @nickvergessen

Thank you for the bounty. Can you also Issue the bounty on #1358977?

Thanks again.

ctulhu posted a comment. Mar 8th (9 months ago)

Hi! Im planning to disclose this.

Can you redact the result of `sudo -u www-data php occ config:list system`?

Thanks.

nickvergessen Nextcloud staff posted a comment. Mar 9th (9 months ago)

I redacted everything that I think is sensible, mind to check?

ctulhu posted a comment. Mar 9th (9 months ago)

Thanks @nickvergessen Its good.

Will there be a CVE for this?

nickvergessen Nextcloud staff posted a comment. Mar 21st (8 months ago)

Hi there, I'm currently on-boarding new colleagues to the process. it will just take a little more time ~1-2 weeks.
There will be an advisory + CVE as usual.

nickvergessen Nextcloud staff updated the severity from Low to Low (3.5). May 2nd (7 months ago)

nickvergessen Nextcloud staff posted a comment. May 2nd (7 months ago)

We plan to release public advisories for this issue on 19.05.2022. We've added a draft version of the advisory as summary to this report: https://github.com/nextcloud/security-advisories/security/advisories/GHSA-hx9w-xfrg-2qvp

Please let us know if you wish any changes to the advisory.

nickvergessen Nextcloud staff updated CVE reference to CVE-2022-24906. May 5th (7 months ago)

○ ctulhu agreed to disclose this report. May 20th (6 months ago)

○ This report has been disclosed. May 20th (6 months ago)