

New issue

[Jump to bottom](#)

TOTP Generate Recovery Codes MFA #965

✓ Closed tahussle opened this issue on Aug 30 · 1 comment

tahussle commented on Aug 30

Area

Web Client MFA /web/client/mfa

Summary

Not sure if this is the expected behaviour, but a user required to use MFA has the option to generate recovery codes even before configuring and enabling it on account . This option is available after logging in with username / password. This means an attacker that knows the user's password could potentially generate a bunch of recovery codes bypassing 2FA after it enabled on account at a later date.

Steps to reproduce as Admin

As an Admin create a new account for a user with a password but enable requirement for MFA.

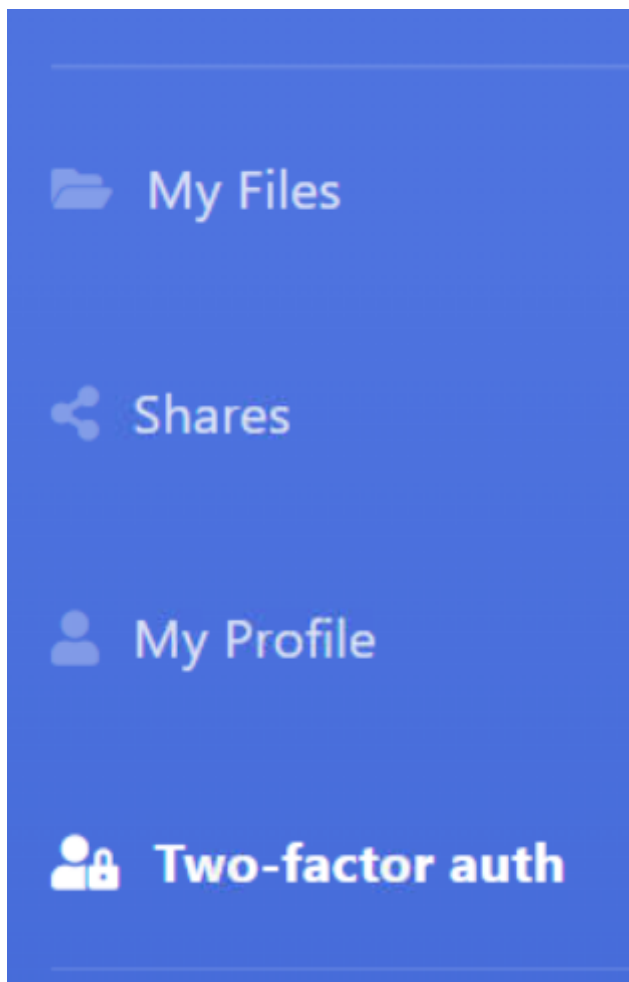
Steps to reproduce the behavior user:

The user logs into the webclient and will get this page

Forbidden

Two-factor authentication requirements not met, please configure two-factor authentication for the following protocols: HTTP

on all other options when the user clicks they get image above



Scroll to bottom and click Generate codes and store it for later.

Recovery codes

Recovery codes are a set of one time use codes that can be used in place of the TOTP to login to the web UI. You can use them if you lose access to your phone to login to your account and disable or regenerate TOTP configuration.

To keep your account secure, don't share or distribute your recovery codes. We recommend saving them with a secure password manager.

View

If you generate new recovery codes, you automatically invalidate old ones.

Generate

After enable 2FA

Expected behavior

Options to generate codes should not be visible until 2FA has been enabled on account i would have thought?

Require two-factor auth for

HTTP

Update protocols

Configuration

Default

Generate new secret

System info :

OS Name: Redhat

OS Version: 9

sftpgo version: SFTPGO 2.3.3-665016e-2022-08-05T08:54:48Z +metrics +azblob +gcs +s3 +bolt +mysql

+pgsql +sqlite +portable

sftpgo install source: Yum

 **drakkan** closed this as completed in [58311ab](#) on Aug 31

 **drakkan** added a commit that referenced this issue on Aug 31

 MFA: allow recovery codes only if two-factor auth is enabled ...

✓ 3267a50

 **drakkan** added a commit that referenced this issue on Aug 31

 MFA: allow recovery codes only if two-factor auth is enabled ...

✓ c304143

drakkan commented on Sep 1

Owner

Thanks!

  **GoVulnBot** mentioned this issue on Sep 2

x/vulndb: potential Go vuln in github.com/drakkan/sftpgo: CVE-2022-36071

[golang/vulndb#964](#)

✓ Closed

Assignees

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

