New issue

Jump to bottom

Rclone generating weak passwords - CVE-2020-28924 #4783

Closed ncw opened this issue on Nov 18, 2020 · 0 comments

Labels bug security

Milestone v1.54

ncw commented on Nov 18, 2020 • edited Member

Rclone security problem - CVE-2020-28924

Passwords users have generated using `rclone config` with rclone 1.49.0 (released 2019-08-26) to 1.53.2 (released 2020-10-26) may be insecure and should be changed.

Passwords you made up yourself are fine.

This is known as CVE-2020-28924.

There is a tool to check your rclone config file for bad passwords here: https://github.com/rclone/passwordcheck

See this forum post for additional help.

Analysis

In this commit

193c30d

`random.Password` was factored out into `lib/random`.

At that time the library `crypto/rand` was accidentally replaced with `math/rand` leading to the pseudo random number generator being used instead of the crypto strong random number generator.

Consequences:

Callers of `random.Password` will have been getting a password based on `math/rand` instead of `crypto/rand` which reduces the amount of entropy for passwords enormously.

- `fs/config/config.go: Password = random.Password`
  - This is choosing random passwords for users in the config generator.
  - This is a problem since users may have used these to configure services.
- `fs/rc/rcserver/rcserver.go: randomPass, err := random.Password(128)`
  - This is choosing short lived random passwords for use with the web ui.
  - This is a minor problem since these passwords are regenerated every time rclone is run.
- `lib/oauthutil/oauthutil.go: state, err := random.Password(128)`
  - This is making some random state for the oauth callback.
  - This isn't a security problem

Rclone initialised the seed of `math/rand` in cmd/cmd.go Main with

```
rand.Seed(time.Now().Unix())
```

However `time.Now().Unix()` only changes every second, meaning passwords generated only change every second. The passwords generated by `random.Password` are therefore completely determinstic based on the unix second that rclone was started.

Consequences

Passwords users have generated using `rclone config` may be insecure. In particular if you generated a password like this with `rclone config` using rclone 1.49.0 (released 2019-08-26) to 1.53.2 (released 2020-10-26) then it will have been selected from a limited set of passwords and should be changed.

```
Password or pass phrase for encryption.
y) Yes type in my own password
g) Generate random password
y/g> g
Password strength in bits.
64 is just about memorable
128 is secure
1024 is the maximum
Bits> 64 <- the number you typed in here is irrelevant
Your password is: XXXXXXXXXXX
```

Versions

This commit is present in these released version of rclone

- `v1.49.0`
- `v1.49.1`
- `v1.49.2`
- `v1.49.3`
- `v1.49.4`

- v1.49.5
- v1.50.0
- v1.50.1
- v1.50.2
- v1.51.0
- v1.52.0
- v1.52.1
- v1.52.2
- v1.52.3
- v1.53.0
- v1.53.1
- v1.53.2

The faulty commit went into rclone at "Sun Aug 25 08:39:31 2019 +0100"

Fixes

This issue is easily fixed with commit `7985df3`

All uses of `math/rand` were reviewed in the code

An additional commit `f090549` was added to seed the random number generator with a crypto strong seed as a mitigation for any future problems.

Demonstration of the problem

Save this bash script to a file called `test-rclone-password.sh` and make it executable.

```
#!/bin/bash
# Test the password generation of rclone
# optionally pass in a path to an rclone binary to use as the first argument

RCLONE="${1:-rclone}"

# Check the binary exists
if ! ${RCLONE} version >/dev/null 2>&1; then
    echo "Rclone binary ${RCLONE} not found"
    exit 1
fi

(
    # Run through the rclone config generator creating a crypt backend
    echo "n" ; sleep .1
    echo "test" ; sleep .1
    echo "crypt" ; sleep .1
    echo "/tmp" ; sleep .1
    echo "1" ; sleep .1
    echo "1" ; sleep .1
    echo "g" ; sleep .1
    echo "64" ; sleep .1
) | ${RCLONE} config 2>&1 | grep "Your password is"
```

If you run multiple copies of it at once which start at the same second, you can see that with a vulnerable rclone all the passwords generated are the same. Pass it an rclone binary to test (or leave off to use the one on the path)

```
$ ./test-rclone-password.sh rclone-v1.53.2 & ./test-rclone-password.sh rclone-v1.53.2 & ./test-rclone-password.sh rclone-v1.53.2
Bits> Your password is: eULvaUR9A_A
Bits> Your password is: eULvaUR9A_A
Bits> Your password is: eULvaUR9A_A
```

However if this is done with a non vulnerable rclone you will get all different passwords

```
$ ./test-rclone-password.sh rclone-v1.48 & ./test-rclone-password.sh rclone-v1.48 & ./test-rclone-password.sh rclone-v1.48
Bits> Your password is: G5dODi-AoFo
Bits> Your password is: KL1QRvaRSXw
Bits> Your password is: b6sVRzjfdkg
```

Authors

This problem was reported to the rclone team by Victor9. Nick Craig-Wood (**@ncw**) fixed the problem, wrote up the advisory and made the checking tool. Klaus Post (**@klauspost**) reviewed the post and patches.

👍 2

ncw added bug security labels on Nov 18, 2020

ncw added this to the **v1.54** milestone on Nov 18, 2020

ncw added a commit to rclone/passwordcheck that referenced this issue on Nov 19, 2020

`Rclone insecure password checker` ··· `8fab234`

ncw added a commit to rclone/passwordcheck that referenced this issue on Nov 19, 2020

`Rclone insecure password checker` ··· `8217624`

ncw added a commit that referenced this issue on Nov 19, 2020

random: seed math/rand in one place with crypto strong seed #4783 ··· f090549

ncw closed this as completed in 7985df3 on Nov 19, 2020

---

ncw added a commit that referenced this issue on Nov 19, 2020

random: fix incorrect use of math/rand instead of crypto/rand CVE-202… ··· 4c215cc

ncw added a commit that referenced this issue on Nov 19, 2020

random: seed math/rand in one place with crypto strong seed #4783 ··· c8b11d2

ncw changed the title ~~Place holder issue for security issue~~ **Rclone generating weak passwords - CVE-2020-28924** on Nov 19, 2020

x0b mentioned this issue on Nov 19, 2020

Information regarding CVE-2020-28924 x0b/rcx#101

Closed

bob-beck pushed a commit to openbsd/ports that referenced this issue on Nov 20, 2020

Update to rclone-1.53.3 ··· a8d7493

netbsd-srcmastr pushed a commit to NetBSD/pkgsrc that referenced this issue on Nov 20, 2020

rclone: Update to 1.53.3 ··· f3884de

Evernow mentioned this issue on Feb 16, 2021

NEW **Software Suggestion | Rclone** privacytools/privacytools.io#2195

Open

1 task

pchristod mentioned this issue on Jan 26

RClone at v.1.53.0 - Update always to latest version romancin/rclonebrowser-docker#35

Closed

Assignees

No one assigned

Labels

bug security

Projects

None yet

Milestone

v1.54

Development

No branches or pull requests

1 participant