

New issue

[Jump to bottom](#)

## [security] Any password unlocks tomb when using pinentry-curses and non-empty \$DISPLAY #385

🔒 Closed

aaronjanse opened this issue on Nov 3, 2020 · 12 comments · Fixed by #386

Assignees



aaronjanse commented on Nov 3, 2020

Contributor

Thank you for this tool. I've been using it for a while, and I appreciate its straightforwardness.

I recently noticed that my tomb unlocks no matter what password is provided.

Steps to reproduce:

1. Use `tomb` with `pinentry-curses` in the `$PATH`
2. Run `tomb dig -s 100 foobar`
3. Provide any password for `tomb forge foobar.key`
4. Provide any password for `tomb lock foobar -k foobar.key`
5. Provide any password for `tomb open foobar -k foobar.key (!!!)`

My operating system is NixOS.

jaromil commented on Nov 3, 2020

Member

@aaronjanse weird, can you give us the output of `tomb -v`

aaronjanse commented on Nov 3, 2020

Contributor Author

```
$ tomb -v
Tomb 2.7 - a strong and gentle undertaker for your secrets

Copyright (C) 2007-2017 Dyne.org Foundation, License GNU GPL v3+
This is free software: you are free to change and redistribute it
For the latest sourcecode go to <http://dyne.org/software/tomb>

This source code is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
When in need please refer to <http://dyne.org/support>.

System utils:

gpg: WARNING: unsafe permissions on homedir '/home/ajanse/.gnupg'
gpg: WARNING: unsafe permissions on homedir '/home/ajanse/.gnupg'
Sudo version 1.9.3p1
cryptsetup 2.3.4
pinentry-curses (pinentry) 1.1.0
findmnt from util-linux 2.36
gpg (GnuPG) 2.2.23 - key forging algorithms (GnuPG symmetric ciphers):
IDEA 3DES CAST5 BLOWFISH AES AES192 AES256 TWOFISH CAMELLIA128 CAMELLIA192 CAMELLIA256

Optional utils:

/nix/store/vkmmfr10cbz8799yvyw352607jrw92h-gettext-0.21/bin/gettext
dcfldd not found
/run/current-system/sw/bin/shred
steghide not found
/nix/store/zs5ycw09gljk0ay6wsnz70vf47dp9z83-e2fsprogs-1.45.5-bin/bin/resize2fs
tomb-kdb-pbkdf2 not found
gencode not found
swish-e not found
unoconv not found
lsof not found
```

jaromil commented on Nov 3, 2020

Member

@aaronjanse thanks! is there a nixos version we can refer to and perhaps a docker distribution of it to try reproduce?

aaronjanse commented on Nov 4, 2020

Contributor Author

Ah, I'm having trouble finding a NixOS container that contains everything needed for tomb. Is there a known working Docker image that works for tomb that I could modify to use Nix?

Narrat commented on Nov 6, 2020

Contributor

Maybe it is worth to look at the `gpg.conf` and `gpg-agent.conf` ? There was a similar issue, where no pinentry was shown and the tomb was unlocked. Maybe this is similar, but pinentry is shown despite the password of the tomb still being cached?

aaronjanse commented on Nov 8, 2020

Contributor Author

This is my `~/gnupg/gpg-agent.conf`:

```
pinentry-program /nix/store/wfhgv1vb14n1hgflq565z2z8gd1r5b3v-pinentry-1.1.0-gtk2/bin/pinentry
```

I have no `~/gnupg/gpg.conf`.

Narrat commented on Nov 9, 2020

Contributor

Not much :D Curious

Is every pinentry binary in a package of its own? Can the faulty behaviour reproduced with the other pinentry variants?

And could I ask additionally for the result of `tree` for the location `/nix/store/wfhgv1vb14n1hgflq565z2z8gd1r5b3v-pinentry-1.1.0-gtk2` ?

 aaronjanse changed the title ~~(security) Any password unlocks tomb when using pinentry-curses on NixOS~~ [security] On NixOS, any password unlocks tomb when using pinentry-curses on Nov 9, 2020

aaronjanse commented on Nov 9, 2020

Contributor Author

Aha! I think I found it!

This is only happening for `pinentry-curses`, not `pinentry-gtk2`. The password being read is `tomb [W] Detected DISPLAY, but only pinentry-curses is found.`

[Tomb/tomb](#)

Lines 480 to 485 in fb154bb

```
480     if _is_found "pinentry-curses"; then
481         _verbose "using pinentry-curses"
482     else
483         _warning "Detected DISPLAY, but only pinentry-curses is found."
484         output=$(pinentry_assuan_getpass | pinentry-curses)
485     else
```

Perhaps this issue is not specific to NixOS.

aaronjanse commented on Nov 9, 2020

Contributor Author

@Narrat Here's my patch ( `master...aaronjanse:security-pinentry-curses` ). I'm putting it here instead of a PR to decrease visibility.

Note that affected Tomb users will need to use the password `tomb [W] Detected DISPLAY, but only pinentry-curses is found.` to use their tomb after applying the patch.

jaromil commented on Nov 10, 2020 • edited

Member

Awesome! please file a PR, there is no security through obscurity and no reason for us to hide bugs! This will be listed [among other glitches in the history of tomb](#) to facilitate bugtracking. Tomb may be not the best tool out there, but at least its a honest one!

FTR this bug was introduced by my commit [bbe9a49](#) in November 2014 and seems to affect installations where a X11 DISPLAY is available but only `pinentry-ncurses` is installed; I'm not too worried since people using Tomb in this condition will see immediately that their password doesn't works at first test.

 1

aaronjanse commented on Nov 10, 2020

Contributor Author

| Tomb may be not the best tool out there, but at least its a honest one!

Thank you for this! This is why I use Tomb :-)

 1

 aaronjanse mentioned this issue on Nov 10, 2020

Use `_verbose` for `pinentry-curses` in `ask_password` #386

 Merged

 aaronjanse changed the title ~~(security) On NixOS, any password unlocks tomb when using pinentry-curses~~ [security] Any password unlocks tomb when using pinentry-curses and non-empty `$DISPLAY` on Nov 11, 2020


 jaromil self-assigned this on Nov 11, 2020


 jaromil closed this as completed in [#386](#) on Nov 11, 2020

 jaromil mentioned this issue on Nov 13, 2020

Rpi no access to tomb folders after apt update #383

 Closed

 jaromil added a commit that referenced this issue on Nov 13, 2020

 document known bug for password with DISPLAY and pinentry-curses ...

763dbdb

carnil commented on Nov 14, 2020

[CVE-2020-28638](#) appears to have been assigned for this issue.



[aaronjanse](#) mentioned this issue on Nov 17, 2020

tomb: 2.7 -> 2.8 NixOS/nixpkgs#104108

Merged

10 tasks

[68420948](#) mentioned this issue on Nov 18, 2020

CVE-2020-28638, Tomb still vulnerable, issue #385 only hidden by pull request #386 #392

Closed

Assignees

jaromil

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

[Use \\_verbose for pinentry-curses in ask\\_password](#)  
[aaronjanse/Tomb](#)

4 participants

