Appendix

A. Survey Questionnaire

Thank you for participating in our survey. The survey consists of 4 sections and will take about 5–10 minutes. All responses are anonymous. Our research is done by [anonymized for review]. It focuses on the security and privacy related aspects of shared configurations, a.k.a. “dotfiles”. Your response provides valuable information and helps us formulate recommendations on the security of this domain for the open source community. Our findings will be published as a paper. If you want to send us additional feedback, concerns or want to get notified about the results please send us a message at [anonymized for review]

Q1. What do you (mostly) use GitHub for?
○ Private projects
○ Active opensource software development
○ Contributions/Bug fixes
○ Github issue reporting/Discussions
○ School/University projects
○ Other: _______

Q2. How many repositories of your own do you have on GitHub (self-created)?

Q3. How often do you actively use GitHub?
○ every day
○ at least once a week
○ at least once per month
○ at least once per year
○ less than once per year/not regularly

Q4. Do you still actively use the dotfile repository?
○ Yes ○ No

Q5. When did you first start to use dotfiles?
○ 0-5 years ago
○ 5-10 years ago
○ more than 10 years ago

Q6. Did you first/also share them in other ways/platforms — if yes, where?
○ No, I don’t share dotfiles on other platforms
○ Dropbox
○ Other cloud file storage
○ Other cloud version control service (e.g. Gitlab, Bitbucket...)
○ Private server
○ Other: _______

Q7. Do you use a tool/technology to manage your dotfiles? If yes, which one?
○ No tool. (I just manually copy my dotfiles to the right place).
○ Plain git (e.g. the ”bare repo” approach).
○ dotbot
○ chezmoi
○ rcm
○ yadm
○ Other: _______

Q8. How many (approx) of your config files are self-written and how many are copy-pasted from somewhere?
○ all are self-written
○ most are self-written
○ about half are copy-pasted, the other half self-written
○ most are copy-pasted
○ all are copy-pasted

Q9. Why did you share your dotfiles on GitHub?

Q10. How concerned are you about software security in general?
○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7

Q11. How do you rate your experience with software security?
○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7

Q12. Did you think about the security of your dotfile repository?
○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7

Q13. How would you rate the security of your dotfile repository?
○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7

Q14. We found several security & privacy issues across dotfile repositories on GitHub. If you are affected, you have received an email from us with further information. With this knowledge, what are your planned changes to your repository?

Q15. Age
○ 10-19 years ○ 20-29 years ○ 30-39 years
○ 40-49 years ○ 50-59 years ○ 60-69 years
○ 70-79 years ○ over 80 years

Q16. Gender
○ Female ○ Male ○ Other

Q17. Country of residence
○ ... list of countries ...

Q18. Highest educational degree
○ School, no diploma
○ Secondary education (high school)
○ Trade/technical/vocational training
○ Undergraduate education (college or university)
○ Postgraduate education (masters or doctorate)
○ Other: _______

Q19. What is your current occupation?

Q20. How many years of experience do you have in software development (if any)?

B. List of Regular expressions

This section gives a list of additional regular expressions that we used to identify relevant secrets and information in dotfiles repositories.

-
  ```
  description = ‘Email Simple’
  email = \b[a-zA-Z0-9_.+-]+@[a-zA-Z0-9-]
  +\.[a-zA-Z0-9-.]+\b
  ```

-
  ```
  description = ‘Firefox Profile’
  path =mozilla/firefox.*(logins\.json|
  cookies\.sqlite|places\.sqlite)
  ```

-
  ```
  description = ‘Files with credentials’
  file = (?i)(id_rsa|passwd|id_rsa.pub|
  pgpass|pem|key|shadow)
  ```

-
  ```
  description = ‘Thunderbird Profile’
  path = ($|/)\.?thunderbird/
  ```

-
  ```
  description = ‘Crypto Wallet’
  file = wallet\.dat
  ```

-
  ```
  description = ‘Chrome Profile’
  path = config.*/(google-chrome|
  chromium)/
  ```

C. Recruitment Mail

We sent the following recruitment mail to the repository owners. Depending on the issues identified in the dotfiles repository, the e-mail text was modified to enlist all the issues found or to state, “No leaks were found in your repository”, in case of no issues.

Hello *username*,

We are a research team at [anonymized for review] . We are writing you, because you are using GitHub and have a repository with configuration files (dotfiles). We did research on the usage and security of these repositories. We found the following issues with your repository (if any):

- Credentials: Your repository may contain API keys or authentication credentials, which(if valid) could be used to log in to web services in your name. RSA Keys: You may have a private key or weak public RSA key, which could be used to authenticate to some service(e.g. via ssh) in your name.
- Private Data: Your repository may contain private data, which is typically not shared publicly. This includes, browsing history, cookies, and chat logs.
- Old/Outdated Dependencies: Your repository may contain software dependencies, which are outdated or misspelled. These could, if installed somewhere, contain security vulnerabilities.

In order to better understand how and why you use shared configurations, we designed a small survey. We would be very happy, if you filled it out. It takes about 10-15 minutes.

link to the survey

If you have any additional notes, questions or feedback, you can reply to this email. Thank you for your time.

Best regards,

[anonymized for review]