New issue

Jump to bottom

Security risk with untrusted repositories (CVE-2022-42906) #45

Open **jcharaoui** opened this issue on Oct 2 · 3 comments

jcharaoui commented on Oct 2 Collaborator

When `powerline-gitstatus` is enabled on the shell and a malicious repository is cloned on the system, simply entering the directory can lead to the execution of arbitrary commands. This risk is documented here: https://blog.sonarsource.com/securing-developer-tools-git-integrations/

We should implement the notion of trusted directories for this plugin, so that `git status` & friends are only executed known-good locations, as opposed to any location on any filesystem.

jcharaoui commented on Oct 9 • edited Collaborator Author

The issue is identical to the one identified for the fish shell:

- Navigating to a compromised git repository may lead to arbitrary code exection
- CVE-2022-20001

jcharaoui added a commit that referenced this issue on Oct 9

`Fix command injection via malicious repository config` ... `fe8e963`

jcharaoui commented on Oct 9 Collaborator Author

Related PR: #46

jcharaoui changed the title ~~Security risk with untrusted repositories~~ **Security risk with untrusted repositories (CVE-2022-42906)** on Oct 13

jcharaoui commented on Oct 13 Collaborator Author

A CVE number has been assigned for this bug: CVE-2022-42906

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant