Fix #25650 - Fix Command Injection in PDB Name - rabin2 #25651

Merged **trufae** merged 1 commit into `radareorg:master` from `jakelamberson:pdb-vuln-fix`

3 weeks ago

jakelamberson commented 3 weeks ago • edited — Contributor

- [x] Mark this if you consider it ready to merge

- [ ] I've added tests (optional)
- [ ] I wrote some lines in the book (optional)

Description

This fixes my vulnerability disclosure.

r_str_escape_sh assumes that the resulting string will be surrounded by double quotes when consumed. This properly uses double quotes.

This is a simple hotfix. For a more robust fix, these PDB filenames should be subject to a character whitelist and `curl` should not be invoked with `system`. I am happy to contribute that later.

`Fix URL command injection in curl PDB download` ··· ✓ `6bb9d15`

trufae merged commit `9236f44` into `radareorg:master` 3 weeks ago

46 checks passed

View details

trufae commented 3 weeks ago — Collaborator

Thanks for the prompt report and fix, yes please, provide the rest of patches and a wider analysis of other similar bugs in the callers for the escape shell function

Reviewers

No reviews

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

Vulnerability Disclosure: Command Injection via Crafted File - rabin2

2 participants