New issue

Vulnerability Disclosure: Command Injection via Crafted File - rabin2 #25650

Closed #25651

jakelamberson opened 3 weeks ago Contributor

Environment

Wed Mar 25 09:33:52 PM EDT 2026
radare2 6.1.3 +35517 abi:78 @ linux-x86_64
birth: git.6.1.2-51-g37ed71413e 2026-03-25__20:58:50
commit: `37ed714`
options: gpl -O? cs:5 cl:2 make
Linux x86_64

Built using `sys/user.sh`

Description

Per `SECURITY.md`, I am disclosing this vulnerability publicly as a Github issue.

There is a command injection vulnerability in the PDB HTTPS download path used by `rabin2 -PP` on non-SSL Unix builds. This is the default build configuration.

Commit `01ca2f6` added a `curl`-based fallback mechanism to download PDBs without a linked SSL. In that path, attacker-controlled PDB filename data flows into a URL, the URL is embedded into a shell command, and that command is executed via `r_sys_cmd()`.

The sanitization performed by `r_str_escape_sh` requires the resulting string to be surrounded by double quotes, which is not the case in socket_http.c.

Using a single quote breaks the shell encapsulation and allows arbitrary command execution.

Test

I am happy to privately provide a crafted sample to a maintainer.

Publicly, the minimal reproduction is:

1. Build radare2 in a configuration where `HAVE_LIB_SSL=0`.
2. Run `rabin2 -PP` on a crafted PE whose PDB filename contains a section enclosed in single quotes, like `evil' ; <malicious commands> ; echo '.pdb`
3. Observe that the injected shell command executes during the HTTPS PDB fetch.

See my pull request.

jakelamberson mentioned this 3 weeks ago

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

trufae closed this as completed in #25651 3 weeks ago

trufae added a commit that references this issue 3 weeks ago

`Fix #25650 - Command injection in curl PDB download ##crash` ··· Verified `9236f44`

Metadata

Assignees

No one assigned

Labels

No labels

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Fix #25650 - Fix Command Injection in PDB Name - rabin2
radareorg/radare2
6.1.4 Latest

Participants