New issue

[Security] Command injection caused by lack of sanitization of PDB symbol names #25730

Closed #25731

jro-calif opened 2 weeks ago · edited by jro-calif Edits Contributor

Environment

```
Mon  6 Apr 2026 14:32:51 +08
radare2 6.1.3 +3 abi:82 @ darwin-arm_64
birth: git.6.1.3 2026-04-06__14:21:39
commit: bdfbf8756562795aec5c53f720d540884a7551d9
options: gpl -O2 cs:5 cl:2 make
Darwin arm64
```

Description

A command injection vulnerability exists in the PDB parser's `print_gvars()` function. When PDB global symbols are emitted in RAD mode, the raw symbol name from PDB binary data is interpolated into an `fN` (flag rename) command without sanitization. Because the standard `idp` command internally executes `.idpi*` (which runs RAD output as r2 commands), an attacker-crafted PDB file can achieve arbitrary command execution.

Root cause

Vulnerable code

```
// filtered_name is sanitized via r_name_filter_dup()
filtered_name = r_name_filter_dup (r_str_trim_head_ro (name));
// filtered_name used in flag creation
pdb->cb_printf ("f pdb.%s = 0x%" PFMT64x " # %d %.*s\n", filtered_name, ...);
```

```
// Raw `name` from PDB binary, NOT sanitized! Vulnerability occurs here!
pdb->cb_printf ("\"fN pdb.%s %s\"\n", filtered_name, name);
```

Thus, by injecting a symbol name containing newlines, the `fN` command can be escaped, thereby resulting in arbitrary command execution when the result of `idpi` is executed.

Test

PoC `.pdb` files are available on request.

Reproduction steps:

1. Produce `target.exe` which links to `debug.pdb`
2. `r2 target.exe`
3. Execute `idp` command

PoC

Screen.Recording.2026-04-06.at.2.31.01.PM.mov

Fix

See #25731

jro-calif added 3 commits that reference this issue 2 weeks ago

`Base64 encode PDB realnames before use in r2 command` ··· Verified `dd94c5c`

`Fix radareorg#25730 - Base64 encode PDB realnames before use in r2 co.` ··· Verified `4a816c4`

`Fix radareorg#25730 - Base64 encode PDB realnames before use in r2 co.` ··· Verified `1549f96`

jro-calif mentioned this 2 weeks ago

Fix #25730 - Base64 encode PDB realnames before use in r2 command #25731

trufae closed this as completed in #25731 2 weeks ago

phix33 added a commit that references this issue 2 weeks ago

`Fix radareorg#25730 - command injection in pdb loading realnames ##se.` ··· Verified `0e38152`

Metadata

Assignees

No one assigned

Labels

No labels

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Fix #25730 - Base64 encode PDB realnames before use in r2 command
radareorg/radare2

6.1.4 Latest

Participants