New issue

Jump to bottom

Vulnerability? Bug? Null write in the get_cmdln_options function in src/options.c. #26

Closed **decentL** opened this issue on Apr 27, 2020 · 5 comments

Labels bug help wanted

decentL commented on Apr 27, 2020

Hi,

In src/options.c, line 337.

```
// malloc() may fail, and str will be NULL.
str=(char*)malloc(strlen(pwd_entry->pw_dir)+14);
// write to Null
snprintf(str,strlen(pwd_entry->pw_dir)+14,"%s/.bwm-ng.conf",pwd_entry->pw_dir);
```

I think this is a vulnerability, and maybe we can patch it as following?

```
str=(char*)malloc(strlen(pwd_entry->pw_dir)+14);
if(!str) return
```

Thanks for any consideration!

Peiyu Liu,
NESA lab,
Zhejiang University

 **vgropp** added bug help wanted labels on Apr 30, 2020

vgropp commented on Apr 30, 2020 Owner

it should terminate with an error and not just return and continue

ofalk commented on Jul 27, 2020 — Contributor

Under which circumstances do you think malloc() can fail and how can one easily reproduce the behaviour?

ofalk mentioned this issue on Jul 27, 2020

Fix potential write to unallocated memory. #27

Merged

vgropp commented on Sep 13, 2020 — Owner

I think https://www.quora.com/What-are-the-possible-ways-malloc-might-fail-Consider-malloc-code-doesnt-have-any-bugs sounds like a wrap up
but it will be not very easy to reproduce it

vgropp closed this as completed in 9774f23 on Sep 29, 2020

---

ofalk commented on Sep 29, 2020 — Contributor

Thx for merging!

vgropp commented on Sep 29, 2020 — Owner

Thx for contributing!

Assignees

No one assigned

Labels

bug help wanted

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants