

[New issue](#)[Jump to bottom](#)

get cpuprof and get memprof commands exist symlink-attacks vulnerability. #4484

 Closed

toptotu opened this issue on Feb 7, 2021 · 6 comments

Assignees



toptotu commented on Feb 7, 2021

Dear beego Team,

I would like to report a security vulnerability in Beego's admin module.

The vulnerability code is in the profile.go file, MemProf and GetCPUProfile function does not correctly check whether the created file exists. As a result, Attackers can launch attacks symlink attacks locally.

poc code:

https://play.golang.org/p/TAvgghgm_7fY

```
func main() {
    file, err := os.Create("cpu-pid.pprof")
    if err != nil {
        fmt.Printf("Error creating file: %s", err)
    }
    _, err = file.Write([]byte("My logs for this process"))
    if err != nil {
        fmt.Println(err)
    }
}
```



```
$ ln -s other/logs cpu-pid.pprof
$ go build symlink_attack.go
$ ./symlink_attack
$ cat other/logs
```

- My logs for this process
- ```
$
```

  toptotu changed the title ~~The /proc interface parameter of the admin service is get cpuprof and get memprof commands, which have a symlink-attacks vulnerability.~~ get cpuprof and get memprof commands, which have a symlink-attacks vulnerability. on Feb 7, 2021

  toptotu changed the title ~~get cpuprof and get memprof commands, which have a symlink-attacks vulnerability.~~ get cpuprof and get memprof commands exist symlink-attacks vulnerability. on Feb 7, 2021

  flycash self-assigned this on Feb 7, 2021

  flycash added **kind/bug** **priority/P0** labels on Feb 7, 2021

flycash commented on Feb 10, 2021

Collaborator

From my understanding, if attackers could run `ln -s other/logs cpu-pid.pprof`, they could do something more dangerous.

toptotu commented on Feb 18, 2021

Author

From my understanding, if attackers could run `ln -s other/logs cpu-pid.pprof`, they could do something more dangerous.

Exactly. Attackers can use this vulnerability to escalate privileges.

flycash commented on Feb 19, 2021

Collaborator

Exactly. Attackers can use this vulnerability to escalate privileges.

I am still confused.

Attackers ran `ln -s other/logs cpu-pid.pprof` and we output the profile data into this file, how did they escalate privileges.

I mean why they don't do something more dangerous directly instead of running `ln -s other/logs cpu-pid.pprof`?

toptotu commented on Feb 20, 2021

Author

Exactly. Attackers can use this vulnerability to escalate privileges.

I am still confused.

Attackers ran `ln -s other/logs cpu-pid.pprof` and we output the profile data into this file, how did they escalate privileges.

I mean why they don't do something more dangerous directly instead of running `ln -s other/logs cpu-pid.pprof`?

What I mean is that in special scenarios, there are unauthorized attacks. The beego application runs under the root permission, and the written pprof file can be created by a low-privilege user using the symlink method, which may cause unauthorized rewriting.

flycash commented on Feb 20, 2021

Collaborator

Got it.

flycash commented on Apr 6, 2021

Collaborator

There are many similar cases in Beego. For example, the log files. So I think we don't need to do more things about it because if we want to enhance this, we should enhance all similar cases. More importantly, I think users should be responsible for ensuring that their server are safe :( I don't have any good idea to resolve this problem.

 flycash closed this as completed on Apr 6, 2021

  flycash removed `priority/P0` `kind/bug` labels on Jun 16

  julieqiu mentioned this issue on Aug 22

x/vulndb: potential Go vuln in [github.com/beego/beego](https://github.com/beego/beego): GHSA-2v6v-q994-xvxx golang/vulndb#575

 Closed

Assignees

 flycash

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants