gphper / ginadmin Public

<> Code

• Issues 2

11 Pull requests

Actions

Security

New issue

Jump to bottom

Read Any File Vulnerability #9



OclickjackingO opened this issue on May 4 · 2 comments

OclickjackingO commented on May 4

Vulnerability file address

internal/controllers/admin/setting/adminSystemController.go line 135 c.Query("path") The incoming path value is not filtered, resulting in arbitrary file reading

```
filePath := gstrings.JoinStr(configs.RootPath, c.Query("path"))
fi, err := os.Open(filePath)
if err != nil {
        con.ErrorHtml(c, err)
        return
}
```

POC

http://ip:port/admin/setting/system/view?

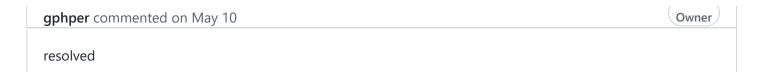
Attack results pictures

image-20220504190918936

gphper added a commit that referenced this issue on May 7

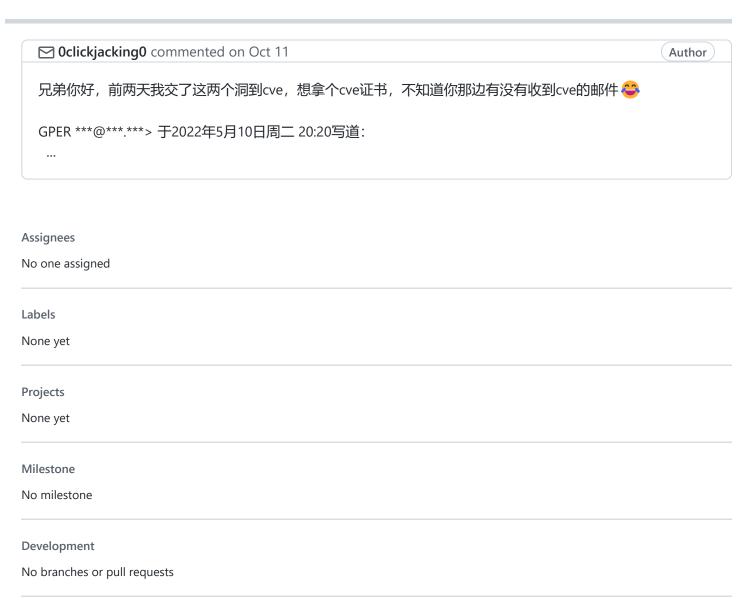
🔼 fix:issues #8 #9

✓ 726109f





oclickjacking0 closed this as completed on Jun 9



2 participants



