**DWR 2000M 5G (CPE) Multiple Security Vulnerability**



**09-Feb-2024**

|  |  |
| --- | --- |
| **Submitted By** |  |
| **Vinod Kumar Shrimalii (mrnmap)**  **Nayab Keshodwala (NK)** |  |

**NAME OF AFFECTED PRODUCT(S) AND VERSION(S)]**

**Model:** DLink DWR 2000M 5G CPEWith Wifi 6 Ax1800

**Version:** DWR-2000M\_1.34ME

1. **Command Injection Vulnerability in Dlink 5G CPE Diagnostics Utility. CRITICAL**

During an examination of the Dlink 5G CPE firmware, A critical security vulnerability has been identified in the "Diagnostics" utility page of the Dlink 5G CPE firmware. Which leads to command injection. This vulnerability allows malicious actors to execute arbitrary system commands through the user input field, compromising the device's integrity and exposing it to various security risks. While functionalities such as ping and traceroute are intended for legitimate network diagnostics, the lack of robust security controls and input validation mechanisms allows for the execution of unauthorized commands, potentially leading to unauthorized access, data extraction, or other malicious activities within the network environment.

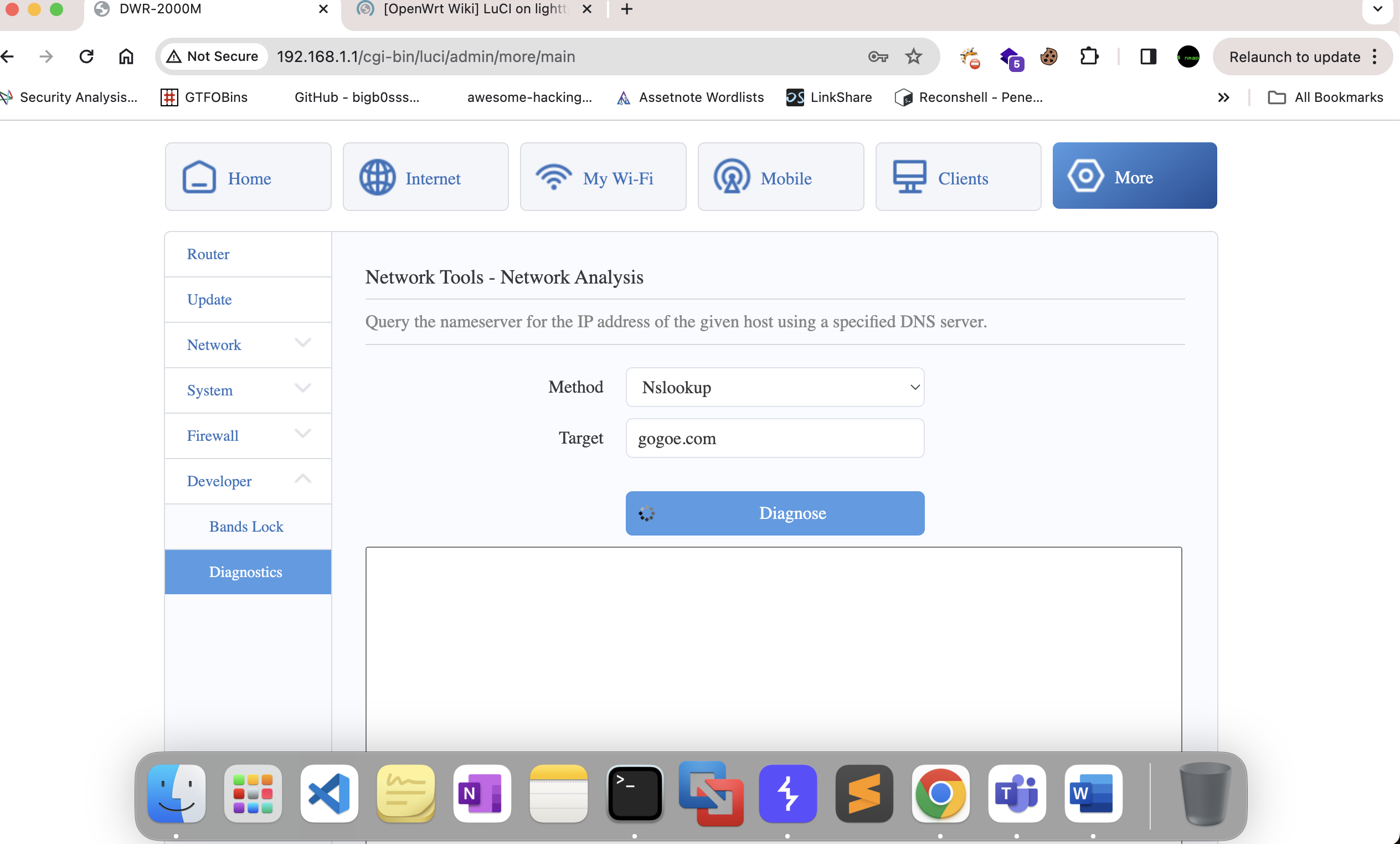
Command Injection is a web security vulnerability that allows attackers to execute arbitrary commands on a server through a vulnerable application. Typically found in web applications that execute system commands based on user input, attackers can manipulate input fields to inject malicious commands, potentially gaining unauthorized access to the server, extracting sensitive data, or causing other harmful actions. Proper input validation, parameterized queries, and least privilege principles are essential for mitigating command injection vulnerabilities.

**Recommendation**

* **Input Validation and Command Whitelisting:**Implement rigorous input validation mechanisms to sanitize user-provided commands effectively. Employ a command whitelisting approach to restrict executed commands solely to known and authorized functionalities, such as ping and traceroute. Reject any input that does not adhere to the predefined whitelist, preventing the execution of unauthorized commands.

**Command Injection Vulnerability in Dlink 5G CPE Diagnostics Utility -POC**

* Network Diagnostics utility for troubleshoot!

****

* Terminating lookup command and supply arbitrary command.

