**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

**Date: 09 Feb-2024**

**Description**

The new DWR-2000M 5G customer premise equipment (CPE) serves as a powerful networking focal point for homes and offices. The DWR-2000M CPE integrates LTE Advanced standard, which combines with leading-edge 5G to dramatically elevate connection speeds. Wi-Fi 6 innovation provides users with simultaneous and seamless access to voice, data and video content. Additional product specifications include.

1. **Telnet Service open Allow Root access to Device CRITICAL**

During a comprehensive security assessment, a critical vulnerability was identified on the CPE (Customer Premises Equipment) device. It was observed that the Telnet service option was enabled, allowing access to the device's internal system. Upon accessing Telnet at port 23 with the device's IP address, unauthorized users were able to gain direct access to the CPE's internal system with root privileges.

**Recommendation**

* Firmware Update: Immediately initiate a firmware update for the CPE device to the latest version provided by the manufacturer. Ensure that this update includes security patches and fixes for known vulnerabilities, in addition to the removal of Telnet and SSH options.
* Dashboard Modification: Modify the dashboard interface of the CPE device to remove any options related to Telnet and SSH access. This prevents users from enabling these potentially insecure remote access methods.
* Default Configuration: Ensure that the default configuration of the CPE device does not include Telnet or SSH options. Any new installations or factory resets should adhere to this configuration to maintain security standards.