**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. **Reflected Cross Site Scripting XSS HIGH**

A critical security vulnerability has been identified in the file upload feature of the VPN configuration module, where insufficient MIME type and file name validation expose the application to Stored Cross-Site Scripting (XSS) attacks. Exploiting this vulnerability, an attacker could upload a malicious OpenVPN configuration file (.ovpn) containing an XSS payload embedded within the file name. For instance, by naming the file "<img src=x onerror=prompt(1)>.ovpn", the attacker triggers the execution of arbitrary JavaScript code when the file name is rendered on the application's interface or logs, leading to a XSS attack.

*Recommendation is same as Stored one*

**Reflected Cross Site Scripting XSS -POC**

* Creating file with following file name <img src=x onerror=prompt (1)>. ovpn and same payload

A screenshot of a computer

Description automatically generated

* Goto VPN section and click on OpenVPN and edit config then upload file based on step 1.

*A screenshot of a computer

Description automatically generated*

* *In Result we got reflected XSS*

*A screenshot of a computer

Description automatically generated*