مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Actively Exploited Vulnerability in DrayTek Routers

Tracking #:432317283

Date:19-05-2025



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a remote code execution vulnerability has been identified in the web management interface of DrayTek Vigor2960 and Vigor300B routers.

## TECHNICAL DETAILS:

A remote code execution vulnerability has been identified in the web management interface of DrayTek Vigor2960 and Vigor300B routers running firmware version 1.5.1.4. The flaw lies within the CGI script /cgi-bin/mainfunction.cgi/apmcfgupload where improper handling of the session parameter allows attackers to perform OS command injection.

Successful exploitation can be achieved remotely and without authentication, potentially allowing attackers to execute arbitrary commands on the router's underlying operating system, compromising device integrity and exposing internal networks.

The vulnerability has been publicly disclosed, and proof-of-concept (PoC) exploits are available, increasing the likelihood of widespread exploitation in the wild.

**Vulnerability Details**

- CVE ID: CVE-2024-12987
- Severity: High (CVSS v3.1: 7.3)
- Affected Products:
    - DrayTek Vigor2960 (Firmware 1.5.1.4 and earlier)
    - DrayTek Vigor300B (Firmware 1.5.1.4 and earlier)
- Vulnerable Component: Web Management Interface
- Vulnerability Type: OS Command Injection (CWE-77, CWE-78)
- Attack Vector: Remote, unauthenticated
- Exploit Availability: Publicly available; active exploitation reported
- Fixed Version: 1.5.1.5 and later

## RECOMMENDATIONS:

- Patch all affected DrayTek Vigor2960 and Vigor300B devices to fixed firmware version or later without delay.
- Limit access to the web management interface to trusted IP addresses using firewall rules or IP whitelisting.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://www.cve.org/CVERecord?id=CVE-2024-12987