مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerabilities in DrayTek Vigor Routers

Tracking #:432316948

Date:07-03-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed security researchers has uncovered multiple critical vulnerabilities in DrayTek Vigor routers, widely used in small office/home office (SOHO) environments.

TECHNICAL DETAILS:

Security researchers has uncovered multiple critical vulnerabilities in DrayTek Vigor routers, widely used in small office/home office (SOHO) environments. These vulnerabilities expose devices to severe risks, including arbitrary code execution, denial-of-service (DoS) attacks, and unauthorized access to sensitive information. Attackers could exploit these flaws to gain complete control over affected devices, potentially leading to data breaches, network compromise, and other malicious activities. Several of these vulnerabilities have been assigned a **CVSS score of 9.8**, indicating their critical severity. Affected models include Vigor165, Vigor2862, Vigor3912, and others, with firmware versions ranging from **3.9.7 to 4.4.5.8**.

Key Vulnerabilities:

1. **CVE-2024-41335 (CVSS 7.5)**: Non-constant time password comparison
   - **Description**: Timing attacks can be used to extract sensitive information due to non-constant time password comparison.
   - **Impact**: Attackers can deduce passwords by analyzing response times.
2. **CVE-2024-41336 (CVSS 7.5)**: Insecure password storage
   - **Description**: Passwords are stored in plaintext, making them accessible to attackers with physical or memory access.
   - **Impact**: Credentials can be easily retrieved, leading to unauthorized access.
3. **Predictable 2FA Code Generation**
   - **Description**: Second-factor authentication codes for WAN login are generated based on boot time, making them predictable.
   - **Impact**: Attackers can bypass 2FA by calculating valid codes.
4. **CVE-2024-41338 (CVSS 7.5)**: DHCP server NULL pointer dereference
   - **Description**: Crafted DHCP requests can trigger a NULL pointer dereference, crashing the DHCP server.
   - **Impact**: Denial-of-service (DoS) attacks can disrupt network operations.
5. **CVE-2024-41339 (CVSS 9.8)**: Undocumented kernel module installation via CGI endpoint
   - **Description**: Attackers can upload crafted kernel modules through the CGI configuration endpoint.
   - **Impact**: Arbitrary code execution with kernel-level privileges.
6. **CVE-2024-41340 (CVSS 8.4)**: APP Enforcement signature update vulnerability
   - **Description**: Attackers can upload arbitrary APP Enforcement signatures to install malicious kernel modules.
   - **Impact**: Arbitrary code execution and system compromise.
7. **CVE-2024-41334 (CVSS 9.8)**: Missing SSL certificate validation for APP Enforcement updates
   - **Description**: SSL certificates are not validated when downloading APP Enforcement signatures, allowing attackers to use non-official servers.
   - **Impact**: Installation of malicious modules and arbitrary code execution.
8. **CVE-2024-51138 (CVSS 9.8)**: TR069 STUN server buffer overflow

- **Description**: A stack-based buffer overflow in the TR069 STUN server's URL parsing can be exploited remotely.
- **Impact**: Arbitrary code execution and complete system compromise.

9. **CVE-2024-51139 (CVSS 9.8)**: CGI POST integer overflow
   - **Description**: An integer overflow in the CGI parser can lead to heap overflows.
   - **Impact**: Arbitrary code execution and system compromise.

Affected Products:
The following DrayTek Vigor router models and firmware versions are affected:

- Vigor165/166: 4.2.7+
- Vigor2620 LTE/VigorLTE 200n: 3.9.8.9+
- Vigor2133/2762/2832: 3.9.9+
- Vigor2135/2765/2766: 4.4.5.1+
- Vigor2860/2862/2925/2926: 3.9.8+ or 3.9.9.5+
- Vigor2865/2866/2927 (LTE/5G): 4.4.5.3+
- Vigor2962/3910: 4.3.2.8+ or 4.4.3.1+
- Vigor3912: 4.3.6.1+

RECOMMENDATIONS:

- Update all affected DrayTek Vigor routers to the latest firmware version provided by DrayTek. Check the official DrayTek website for updates and patches.

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.draytek.com/about/security-advisory/denial-of-service,-information-disclosure,-and-code-execution-vulnerabilities
- https://www.draytek.com/about/security-advisory/buffer-overflow-vulnerabilities-(cve-2024-51138-cve-2024-51139)