مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Command Injection Vulnerability in DrayTek Gateways

Tracking #:432316690

Date:31-12-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability in DrayTek gateway devices that could be exploited to execute malicious code on the affected devices.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-12987**
- CVSS Score 6.9 Medium
- The vulnerability originates from improper input sanitization in the web management interface of the affected devices. Specifically, the /cgi-bin/mainfunction.cgi/apmcfgupload endpoint fails to adequately sanitize the session parameter, enabling attackers to inject malicious commands.
- Successful exploitation of this vulnerability could lead to:
    - Unauthorized command execution
    - Configuration manipulation
    - Sensitive information extraction
    - Further attacks against internal networks
- A proof of concept (PoC) for CVE-2024-12987 publicly available

Affected Devices:

- DrayTek Vigor2960
- DrayTek Vigor300B

Affected Versions:

- Firmware 1.5.1.4 and earlier

Fixed Versions:

- Firmware Version 1.5.1.5 or later

RECOMMENDATIONS:

- **Apply Input Validation**: Ensure all CGI script parameters undergo strict validation and sanitization to mitigate the risk of injection attacks.
- **Restrict Web Interface Access**: Limit access to the web management interface by implementing IP whitelisting for trusted sources.
- **Update Firmware**: Monitor DrayTek's website and support channels for firmware updates addressing this vulnerability. Apply updates promptly once available.

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://nvd.nist.gov/vuln/detail/CVE-2024-12987