



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates- DrayTek

Tracking #:432316374

Date:08-10-2024

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 INTELLIGENCE 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 that DrayTek has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

DrayTek has identified and addressed multiple vulnerabilities in their products. These vulnerabilities could be exploited by attackers to gain unauthorized access to affected devices, steal sensitive information, or disrupt critical services.

Vulnerabilities Details:

- Cross-Site Scripting (XSS), Denial of Service (DoS), and Remote Code Execution:**
 - CVEs:** CVE-2024-41583, CVE-2024-41596
 - Successful exploitation could allow an attacker to execute arbitrary code on the affected device, potentially leading to data theft, unauthorized access, or other malicious activities. Additionally, these vulnerabilities could be used to trigger denial-of-service (DoS) conditions."
- Buffer Overflow Vulnerabilities:**
 - CVEs:** CVE-2024-46550, CVE-2024-46568, CVE-2024-46571, CVE-2024-46580, CVE-2024-46586, CVE-2024-46588, CVE-2024-46598
 - These vulnerabilities could allow an authenticated attacker to trigger a DoS condition by sending specially crafted input.

Note: Refer to Draytek Advisory for Affected Products, Fixed Versions and more information.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by DrayTek.

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/buffer-overflow-vulnerability>
- <https://www.draytek.com/about/security-advisory/cross-site-scripting,-denial-of-service-and-remote-code-execution-vulnerabilities>