



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerability in Western Digital My Cloud Devices

Tracking #:432316346

Date:01-10-2024

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 a critical vulnerability, designated as CVE-2024-22170, has been identified in Western Digital's My Cloud devices, affecting multiple models.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-22170**
- **CVSS Score:** 9.2 (**Critical**)
- This vulnerability allows attackers to execute arbitrary code through an unchecked buffer in the Dynamic DNS client. Exploitation can occur via a Man-in-the-Middle (MitM) attack, where attackers intercept Dynamic DNS update requests and inject malicious payloads, resulting in a buffer overflow

Affected Products:

- My Cloud EX2 Ultra, My Cloud EX4100, My Cloud PR2100, My Cloud PR4100, My Cloud, My Cloud Mirror G2, My Cloud EX2100, My Cloud DL2100, My Cloud DL4100, and WD Cloud.

Fixed Versions:

- My Cloud OS 5 Firmware version 5.29.102

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update Firmware to the latest version.

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.westerndigital.com/support/product-security/wdc-24005-western-digital-my-cloud-os-5-firmware-5-29-102>