مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Moxa Ethernet Switches

Tracking #:432318359

Date:06-02-2026

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 critical vulnerability in Moxa Ethernet switches that could allow bypassing access controls and gaining unauthorized access to the devices.

TECHNICAL DETAILS:

Moxa has identified a critical-severity authentication bypass vulnerability affecting multiple Ethernet switch product lines. The vulnerability exists in the frontend authorization logic and may allow unauthenticated remote attackers to bypass authentication controls.
Successful exploitation could enable attackers to perform brute-force attacks to guess valid credentials or exploit MD5 collision weaknesses to forge authentication hashes, potentially leading to unauthorized access and compromise of affected devices.

Vulnerability Details

- **CVE-2024-12297**
- **CVSS v4.0 Base Score:** 9.2 (Critical)
- **Vulnerability Type:** Frontend Authorization Logic Disclosure / Authentication Bypass
- The vulnerability is caused by flaws in the implementation of the authorization mechanism within the web-based management interface. Although both client-side and back-end verification are present, weaknesses in the authorization logic may allow attackers to bypass authentication checks.
- An attacker could exploit this issue remotely to conduct credential brute-force attempts or perform MD5 collision attacks to generate forged authentication hashes, resulting in unauthorized access to the device and potential compromise of confidentiality, integrity, and availability.

Affected Products

TN-A Series

- TN-4500A Series
- TN-5500A Series
    - Firmware v4.1 and earlier

TN-G Series

- TN-G4500 Series
- TN-G6500 Series
    - Firmware v5.5 and earlier

Fixed Versions

- TN-A, TN-4500A, TN-5500A Series: Firmware v3.13.255
- TN-G, TN-G4500, TN-G6500 Series: Firmware v5.5.255

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by MOXA.

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.moxa.com/en/support/product-support/security-advisory/mpsa-241409-cve-2024-12297-frontend-authorization-logic-disclosure-vulnerability-in-ethernet-switches