مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Moxa PT Switches

Tracking #:432316973

Date:14-03-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Moxa PT Switches. This vulnerability could allow attackers to bypass authentication mechanisms and gain unauthorized access to devices.

TECHNICAL DETAILS:

Moxa has identified a critical vulnerability, CVE-2024-12297, affecting multiple models of its PT Series industrial Ethernet switches. This vulnerability allows attackers to bypass authentication mechanisms, potentially granting unauthorized access to device configurations and disrupting critical services. The flaw resides in the authorization process, enabling brute-force attacks and MD5 collision attacks to compromise device security.

Vulnerability Details:

- CVE-2024-12297
- **CVSS 4.0 Base Score:** 9.2 (Critical)
- An authentication bypass vulnerability exists due to flaws in the authorization mechanism of affected Moxa PT Series switches. Despite client-side and back-end server verification, attackers can exploit weaknesses in its implementation. This allows for brute-force attacks to guess valid credentials or MD5 collision attacks to forge authentication hashes.
- Successful exploitation of this vulnerability could lead to:
    - Unauthorized access to sensitive device configurations.
    - Disruption of critical industrial network services.
    - Potential compromise of connected industrial control systems.
    - Data exfiltration and manipulation.

Affected Products and Firmware Versions:

- PT-508 Series (Firmware version 3.8 and earlier)
- PT-510 Series (Firmware version 3.8 and earlier)
- PT-7528 Series (Firmware version 5.0 and earlier)
- PT-7728 Series (Firmware version 3.9 and earlier)
- PT-7828 Series (Firmware version 4.0 and earlier)
- PT-G503 Series (Firmware version 5.3 and earlier)
- PT-G510 Series (Firmware version 6.5 and earlier)
- PT-G7728 Series (Firmware version 6.5 and earlier)
- PT-G7828 Series (Firmware version 6.5 and earlier)

RECOMMENDATIONS:

- **Patching:** Contact Moxa Technical Support for patches and apply them immediately.
- **Strong Passwords:** Change default passwords to strong, unique ones.
- **Firmware Updates:** Regularly update firmware to the latest versions.
- **Network Segmentation:** Implement network segmentation to limit access.
- **Network Monitoring:** Monitor network traffic for suspicious activity.

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-241408-cve-2024-12297-frontend-authorization-logic-disclosure-vulnerability-identified-in-pt-switches