مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Moxa PT Switches

Tracking #:432316900

Date: 24-02-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Moxa PT switches that could be exploited to disrupt operations by triggering a system crash or cold start, potentially leading to significant operational downtime in industrial environments.

TECHNICAL DETAILS:

Moxa, a leading provider of industrial networking solutions, has issued a security advisory regarding a critical denial-of-service (DoS) vulnerability affecting multiple models of its PT switches. This vulnerability could allow attackers to disrupt operations by causing a system or service crash.

Vulnerability Details:

- **CVE-2024-9404**
- CVSS score 7.5 High
- The vulnerability arises from **insufficient input validation** in the Moxa service, known as **moxa_cmd**, which is primarily used for deployment purposes. Exploiting this vulnerability enables attackers to trigger a cold start or DoS condition, potentially shutting down affected systems.

Affected Versions:

- **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)

Fixed Versions:

- PT-7728 Series v 3.9.2
- PT-7828 Series v 4.0.4
- PT-G503 Series v 5.3.6
- PT-G510 Series v 6.5.8

RECOMMENDATIONS:

- **Apply the latest patches** provided by Moxa.
- **Restrict network access** to affected PT switches to prevent unauthorized access.
- **Disable unnecessary services**, including moxa_cmd, to reduce the attack surface.
- **Monitor network traffic** for any unusual activity that may indicate an attempted exploitation.

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-240933-cve-2024-9404-denial-of-service-vulnerability-identified-in-multiple-pt-switches