مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Moxa Ethernet Switches

Tracking #:432318236

Date:13-01-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Moxa industrial Ethernet switches that use the OpenSSH component, which could allow remote attackers to execute arbitrary code under certain conditions.

TECHNICAL DETAILS:

A critical security vulnerability, tracked as CVE-2023-38408, has been identified in Moxa Ethernet switches that utilize the OpenSSH component. The vulnerability affects the PKCS#11 functionality in OpenSSH's ssh-agent and may allow unauthenticated remote attackers to execute arbitrary code under specific conditions**.**

Vulnerability Details

- **CVE-2023-38408**
- **CVSS Score:** 9.8 Critical
- The vulnerability is caused by an insecure module search path in OpenSSH's ssh-agent, which may allow an attacker with SSH agent access to load unsafe code and achieve remote code execution (RCE).
- This vulnerability exists due to an incomplete fix for CVE-2016-10009 and can be exploited without authentication or user interaction once the attack conditions are met.

Affected Products

- EDS-G4000 Series
- EDS-4008 / EDS-4009 / EDS-4012 / EDS-4014 Series
- EDS-G4008 / EDS-G4012 / EDS-G4014 Series
  - *Affected Versions:* Firmware v4.1 and earlier
- RKS-G4000 Series
- RKS-G4028 / RKS-G4028-L3 Series
  - *Affected Versions:* Firmware v5.0 and earlier

Fixed Version / Remediation

- EDS Series: Update to firmware v4.1.58
- RKS Series: Update to firmware v5.0.4

RECOMMENDATIONS:

- Apply the latest security patches provided by the vendor as soon as possible.
- Restrict network access to affected devices and allow communication only from trusted sources.
- Avoid direct Internet exposure of OT devices and disable unnecessary services and ports.
- Use secure and encrypted channels for remote access and limit access to authorized users.
- Monitor systems and logs regularly for signs of unauthorized or 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-256261-cve-2023-38408-openssh-vulnerability-in-ethernet-switches