مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Lexmark Printers

Tracking #:432317293

Date:20-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Lexmark printers that could potentially be exploited to execute malicious code on affected devices.

TECHNICAL DETAILS:

Lexmark has identified and addressed a critical security vulnerability, CVE-2025-1127, affecting a broad range of its printer models. This flaw, a combination of Path Traversal and Concurrent Execution vulnerabilities within the embedded web server, could allow an unauthenticated attacker to remotely execute arbitrary code on vulnerable devices.

Vulnerability Details:

- CVE-2025-1127
- **CVSSv3 Base Score:** 9.1 (Critical)
- A combination Path Traversal and Concurrent Execution vulnerability exists within the embedded web server in various Lexmark devices. This allows for remote code execution.
- A successful exploit could enable attackers to:
  - Hijack Lexmark printers remotely
  - Gain unauthorized access to internal networks
  - Steal confidential documents
  - Use compromised devices as pivot points for broader cyber-attacks

Affected Models and Firmware Versions:

- Devices running **firmware version .240.205 or earlier**
- Impacted printer series include, but are not limited to:
  CX950, MX953, CX961, CS963, MS531, CX532, CX930, MX931, MS622, MX421, XM1246, CS720, CX820, CS921, and others.

Fixed Versions:

- Lexmark printer firmware version .240.206 or later

RECOMMENDATIONS:

- Audit all Lexmark devices for affected firmware versions.
- Prioritize firmware updates across all impacted printers.
- Enforce strong administrative credentials on all devices.
- Monitor network logs for unusual activity from printer endpoints.
- Stay updated with Lexmark's security advisories for any new developments

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://nvd.nist.gov/vuln/detail/CVE-2025-1127