مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Remote Code Execution Vulnerability in Lexmark Printers

Tracking #:432318375

Date:10-02-2026

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 untrusted search path vulnerability (CVE-2025-65078) has been identified in the Embedded Solutions Framework affecting a wide range of Lexmark printer and multifunction devices.

TECHNICAL DETAILS:

A critical untrusted search path vulnerability (CVE-2025-65078) has been identified in the Embedded Solutions Framework affecting a wide range of Lexmark printer and multifunction devices. This vulnerability allows unauthenticated remote attackers to execute arbitrary code on affected devices without user interaction. With a CVSSv4 base score of 9.3 (Critical), this represents a severe security risk requiring immediate remediation. Organizations using affected Lexmark devices should prioritize firmware updates to protect against potential exploitation.

Vulnerability Information

- CVE Identifier: CVE-2025-65078
- CVSSv4 Score: 9.3
- Severity: Critical
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None

Technical Description

- An untrusted search path vulnerability exists in the Embedded Solutions Framework implemented across various Lexmark printing devices. This vulnerability stems from the application's improper handling of search paths when loading libraries or executables, allowing an attacker to place malicious code in a location that will be executed by the vulnerable application.
- Impact-Successful exploitation of this vulnerability enables attackers to:
  - Execute arbitrary code remotely on affected devices
  - Gain complete control over compromised devices
  - Potentially pivot to other network resources
  - Exfiltrate sensitive data including print jobs and stored credentials
  - Modify device configurations and firmware
  - Use compromised devices as persistent footholds in corporate networks

Affected Device Families and Firmware Versions

MX/M Series Monochrome Devices:

- MX432, XM3142: MXTCT.250.209 and earlier
- M3250, MS622: MSTGM.250.209 and earlier
- MB2442, MB2546, MB2650, MX421, MX521 series, MX622 series, XM1242, XM1246, XM3250: MXTGM.250.209 and earlier
- M5255, M5265, M5270, MS822, MS824, MS826: MSTGW.250.209 and earlier
- MB2770, MX721 series, MX722, MX725, MX822, MX824, MX826, XM5365, XM5370, XM7355, XM7365, XM7370: MXTGW.250.209 and earlier

- MX953, XM9655: MXTLS.250.209 and earlier
- MX931, XM9335: MXTPM.250.209 and earlier
- M3350, MS632, MS639: MSTSN.250.209 and earlier
- MX532, MX632, XM3346, XM3350: MXTSN.250.209 and earlier

CS/C Series Color Devices:

- CS632, CS639: CSTGV.250.209 and earlier
- CS963: CSTLS.250.209 and earlier
- C4342, C4352, CS730, CS735, CS737: CSTMM.250.209 and earlier
- CS943: CSTPC.250.209 and earlier
- C2240, CS622: CSTZJ.250.209 and earlier
- C4150, CS720, CS725, CS727, CS728: CSTAT.230.506 and earlier
- C9235, CS920, CS921, CS923, CS927: CSTMH.230.506 and earlier
- C6160, CS820, CS827: CSTPP.230.506 and earlier

CX/XC Series Multifunction Color Devices:

- CX532, CX635, XC2335, XC2342: CXTGV.250.209 and earlier
- CX833, CX950, CX951, CX961, CX962, CX963, XC8355, XC9525, XC9535, XC9635, XC9645, XC9655: CXTLS.250.209 and earlier
- CX730, CX735, CX737, XC4342, XC4352: CXTMM.250.209 and earlier
- CX930, CX931, CX942, CX943, CX944, XC9325, XC9335, XC9445, XC9455, XC9465: CXTPC.250.209 and earlier
- CX522, CX622, CX625, MC2535, MC2640, XC2235, XC2240, XC4240: CXTZJ.250.209 and earlier
- CX725, CX727, XC4140, XC4143, XC4150, XC4153: CXTAT.230.506 and earlier
- CX920, CX921, CX922, CX923, CX924, CX927, CX928, XC9225, XC9235, XC9245, XC9255, XC9265: CXTMH.230.506 and earlier
- CX820, CX825, CX827, CX860, XC6152, XC6153, XC8155, XC8160, XC8163: CXTPP.230.506 and earlier

RECOMMENDATIONS:

- Apply Firmware Updates: Download appropriate firmware patches from Lexmark support portal.
- Prioritize internet-facing or publicly accessible devices.

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.lexmark.com/content/dam/support/collateral/security-alerts/CVE-2025-65078.pdf