Lexmark Security Advisory

Revision: 0.4
Last update: 03 February 2026

Summary
An untrusted search path vulnerability has been identified in the Embedded Solutions Framework in various Lexmark devices.

References
CVE: CVE-2025-65078
ZDI: ZDI-CAN-28477
CWE: CWE-426

Details
An untrusted search path vulnerability has been identified in the Embedded Solutions Framework in various Lexmark devices. This vulnerability can be leveraged by an attacker to execute arbitrary code.

CVSSv4 Base Score: 9.3 (AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)

CVSSv4 scores are calculated in accordance with CVSS version 4.0 (https://www.first.org/cvss/v4-0/user-guide).

Impact
Successful exploitation of this vulnerability can lead to an attacker being able to remotely execute arbitrary code on a device.

Affected Products
To determine a device's firmware level, select the "Settings" > "Reports" > "Menu Settings Page" menu item from the operator panel or web interface. If the firmware level listed under "Device Information" matches any level under "Affected Releases," then upgrade to a "Fixed Release."

Lexmark Models	Affected Releases	Fixed Releases
MX432, XM3142	MXTCT.250.209 and previous	MXTCT.250.210 and later
M3250, MS622	MSTGM.250.209 and previous	MSTGM.250.210 and later
MB2442, MB2546, MB2650, MX421, MX521, MX521ade, MX521de, MX522, MX622, MX622ade, MX622adhe, XM1242, XM1246, XM3250	MXTGM.250.209 and previous	MXTGM.250.210 and later
CS632, CS639	CSTGV.250.209 and previous	CSTGV.250.210 and later
CX532, CX635, XC2335, XC2342	CXTGV.250.209 and previous	CXTGV.250.210 and later

M5255, M5265, M5270, MS822, MS824, MS826	MSTGW.250.209 and previous	MSTGW.250.210 and later
MB2770, MX721, MX721de, MX722, MX725, MX822, MX824, MX826, XM5365, XM5370, XM7355, XM7365, XM7370	MXTGW.250.209 and previous	MXTGW.250.210 and later
CS963	CSTLS.250.209 and previous	CSTLS.250.210 and later
CX833, CX950, CX951, CX961, CX962, CX963, XC8355, XC9525, XC9535, XC9635, XC9645, XC9655	CXTLS.250.209 and previous	CXTLS.250.210 and later
MX953, XM9655	MXTLS.250.209 and previous	MXTLS.250.210 and later
C4342, C4352, CS730, CS735, CS737	CSTMM.250.209 and previous	CSTMM.250.210 and later
CX730, CX735, CX737, XC4342, XC4352	CXTMM.250.209 and previous	CXTMM.250.210 and later
CS943	CSTPC.250.209 and previous	CSTPC.250.210 and later
CX930, CX931, CX942, CX943, CX944, XC9325, XC9335, XC9445, XC9455, XC9465	CXTPC.250.209 and previous	CXTPC.250.210 and later
MX931, XM9335	MXTPM.250.209 and previous	MXTPM.250.210 and later
M3350, MS632, MS639	MSTSN.250.209 and previous	MSTSN.250.210 and later
MX532, MX632, XM3346, XM3350	MXTSN.250.209 and previous	MXTSN.250.210 and later
C2240, CS622	CSTZJ.250.209 and previous	CSTZJ.250.210 and later
CX522, CX622, CX625, MC2535, MC2640, XC2235, XC2240, XC4240	CXTZJ.250.209 and previous	CXTZJ.250.210 and later
C4150, CS720, CS725, CS727, CS728	CSTAT.230.506 and previous	CSTAT.230.507 and later

CX725, CX727, XC4140, XC4143, XC4150, XC4153	CXTAT.230.506 and previous	CXTAT.230.507 and later
C9235, CS920, CS921, CS923, CS927	CSTMH.230.506 and previous	CSTMH.230.507 and later
CX920, CX921, CX922, CX923, CX924, CX927, CX928, XC9225, XC9235, XC9245, XC9255, XC9265	CXTMH.230.506 and previous	CXTMH.230.507 and later
C6160, CS820, CS827	CSTPP.230.506 and previous	CSTPP.230.507 and later
CX820, CX825, CX827, CX860, XC6152, XC6153, XC8155, XC8160, XC8163	CXTPP.230.506 and previous	CXTPP.230.507 and later

Obtaining Updated Software
To obtain firmware that resolves this issue or if you have special code, please contact Lexmark's Technical Support Center at http://support.lexmark.com to find your local support center.

Workarounds
Lexmark recommends a firmware update if your device has affected firmware.

Exploitation and Public Announcements
Lexmark is not aware of any malicious use against Lexmark products of the vulnerability described in this advisory.

Lexmark would like to thank the following people working with Trend Micro's Zero Day Initiative (ZDI) for bringing this issue to our attention: Interrupt Labs

Status of this Notice
THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND IS PROVIDED WITHOUT ANY EXPRESS OR IMPLIED GUARANTEE OR WARRANTY WHATSOEVER, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR USE OR PURPOSE. LEXMARK RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

Distribution
This advisory is posted on Lexmark's web site at http://support.lexmark.com/alerts. Future updates to this document will be posted on Lexmark's web site at the same location.

Revision History

Revision	Date	Reason
0.1	07 January 2026	Initial draft
0.2	13 January 2026	Added affected products/releases
0.3	27 January 2026	Updated affected products to include only esf capable devices

0.4	03 February 2026	Corrected CVE number: CVE-2025-65083 to CVE-2025-65078