AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Dobësi Kritike e Ekzekutimit të Kodit nga Distanca në Printerët Lexmark

Data: 10/02/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Është identifikuar një **dobësi kritike e tipit "untrusted search path"** në **Embedded Solutions Framework**, e cila prek një gamë shumë të gjerë printerësh dhe pajisjesh multifunksionale **Lexmark**.
Dobësia, e gjurmuar si **CVE-2025-65078**, i lejon **sulmues të paautentikuar nga distanca** të ekzekutojnë **kod arbitrar** në pajisjet e prekura **pa asnjë ndërveprim nga përdoruesi**. Me një **CVSS v4 Base Score: 9.3 (Kritike)**, kjo përfaqëson një rrezik shumë të lartë sigurie që kërkon **veprime të menjëhershme korrigjuese**.
Organizatat që përdorin pajisje Lexmark të prekura duhet të japin prioritet **përditësimeve të firmware-it** për të parandaluar shfrytëzimin e mundshëm.

Informacione Teknike

Detaje të Dobësisë:

- **CVE ID:** CVE-2025-65078
- **CVSS v4 Score:** 9.3
- **Rrezikshmëria:** Kritike
- **Vektori i sulmit:** Rrjet
- **Kompleksiteti i sulmit:** I ulët
- **Privilegje të kërkuara:** Asnjë
- **Ndërveprim nga përdoruesi:** Asnjë

Ekziston një dobësi *untrusted search path* në **Embedded Solutions Framework** të implementuar në pajisje të ndryshme printimi Lexmark.

Dobësia buron nga trajtimi i pasaktë i rrugëve të kërkimit gjatë ngarkimit të librarive ose ekzekutuesve, duke i lejuar sulmuesit të vendosin kod keqdashës në një lokacion që do të ekzekutohet nga aplikacioni vulnerabël.

Ndikimi

Shfrytëzimi me sukses i kësaj dobësie u lejon sulmuesve të:

- Ekzekutojnë kod arbitrar nga distanca në pajisjet e prekura
- Marrin kontroll të plotë mbi pajisjet e kompromentuara
- Kryejnë lëvizje laterale drejt burimeve të tjera të rrjetit
- Ekfiltrjnë të dhëna sensitive, përfshirë punë printimi dhe kredenciale të ruajtura
- Modifikojnë konfigurimet dhe firmware-in e pajisjes
- Përdorin pajisjet e kompromentuara si pika persistente hyrjeje në rrjetet korporative

Pajisjet e Prekura – Familje dhe Versione Firmware

MX / M Series – Pajisje Monokromatike

- MX432, XM3142: **MXTCT.250.209** dhe më herët
- M3250, MS622: **MSTGM.250.209** dhe më herët
- MB2442, MB2546, MB2650, MX421, MX521 series, MX622 series, XM1242, XM1246, XM3250: **MXTGM.250.209** dhe më herët
- M5255, M5265, M5270, MS822, MS824, MS826: **MSTGW.250.209** dhe më herët
- MB2770, MX721 series, MX722, MX725, MX822, MX824, MX826, XM5365, XM5370, XM7355, XM7365, XM7370: **MXTGW.250.209** dhe më herët
- MX953, XM9655: **MXTLS.250.209** dhe më herët
- MX931, XM9335: **MXTPM.250.209** dhe më herët
- M3350, MS632, MS639: **MSTSN.250.209** dhe më herët
- MX532, MX632, XM3346, XM3350: **MXTSN.250.209** dhe më herët

CS / C Series – Pajisje me Ngjyra

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

CX / XC Series – Pajisje Multifunksionale me Ngjyra

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

Rekomandime

AKSK rekomandon të aplikoni menjëherë përditësimet e firmware-it duke i shkarkuar nga portali zyrtar i mbështetjes Lexmark.

Referenca

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