Lexmark Security Advisory:

Revision: 1.0
Last update: 17 January 2025
Public Release Date: 30 January 2025

Summary

A combination Path Traversal and Concurrent Execution vulnerability exists within the embedded web server in various Lexmark devices.

References

CVE: CVE-2024-11348

ZDI: ZDI-CAN-25848; ZDI-CAN-25849

CWE: CWE-22; CWE-362

Details

A combination Path Traversal and Concurrent Execution vulnerability exists within the embedded web server in various Lexmark devices.
The vulnerability can be leveraged by an attacker to execute arbitrary code.

CVSSv3 Base Score 9.1 (AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)
Impact Subscore: 6.0
Exploitability Subscore: 2.3

CVSSv3 scores are calculated in accordance with CVSS version 3.1 (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator)

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 devices firmware level, select the “Settings”->“Reports”->”Menu Setting Page” menu item from the operator panel. 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
CX950, CX951	CXTLS.240.205 and previous	CXTLS.240.206 and later
XC9525, XC9535	CXTLS.240.205 and previous	CXTLS.240.206 and later
MX953	MXTLS.240.205 and previous	MXTLS.240.206 and later
CX961, CX962, CX963	CXTLS.240.205 and previous	CXTLS.240.206 and later

XC9635, XC9645, XC9655	CXTLS.240.205 and previous	CXTLS.240.206 and later
CS963	CSTLS.240.205 and previous	CSTLS.240.206 and later
CX833	CXTLS.240.205 and previous	CXTLS.240.206 and later
XC8355	CXTLS.240.205 and previous	CXTLS.240.206 and later
MS531, MS631	MSNSN.240.205 and previous	MSNSN.240.206 and later
MS632, M3350	MSTSN.240.205 and previous	MSTSN.240.206 and later
MX532, MX632, XM3350	MXTSN.240.205 and previous	MXTSN.240.206 and later
CS531, C2335	CSNGV.240.205 and previous	CSNGV.240.206 and later
CS632	CSTGV.240.205 and previous	CSTGV.240.206 and later
CX532, CX635, XC2335	CXTGV.240.205 and previous	CXTGV.240.206 and later
CX930, CX931, CX942, CX943, CX944	CXTPC.240.205 and previous	CXTPC.240.206 and later
XC9325, XC9335, XC9445, XC9455, XC9465	CXTPC.240.205 and previous	CXTPC.240.206 and later
CS943	CSTPC.240.205 and previous	CSTPC.240.206 and later
MX432	MXTCT.240.205 and previous	MXTCT.240.206 and later
XM3142	MXTCT.240.205 and previous	MXTCT.240.206 and later
MX931	MXTPM.240.205 and previous	MXTPM.240.206 and later
CX730, CX735, CX737	CXTMM.240.205 and previous	CXTMM.240.206 and later
XC4342, XC4352	CXTMM.240.205 and previous	CXTMM.240.206 and later
CS730, CS735, CS737	CSTMM.240.205 and previous	CSTMM.240.206 and later
C4342, C4352	CSTMM.240.205 and previous	CSTMM.240.206 and later
B2236	MSLSG.230.407 and previous	MSLSG.230.408 and later
MB2236	MXLSG.230.407 and previous	MXLSG.230.408 and later
MS331, MS431, MS439	MSLBD.230.407 and previous	MSLBD.230.408 and later
M1342	MSLBD.230.407 and previous	MSLBD.230.408 and later
B3442, B3340	MSLBD.230.407 and previous	MSLBD.230.408 and later
XM1342	MXLBD.230.407 and previous	MXLBD.230.408 and later
MX331, MX431	MXLBD.230.407 and previous	MXLBD.230.408 and later
MB3442	MXLBD.230.407 and previous	MXLBD.230.408 and later
MS321, MS421, MS521, MS621	MSNGM.230.407 and previous	MSNGM.230.408 and later
M1242, M1246	MSNGM.230.407 and previous	MSNGM.230.408 and later
B2338, B2442, B2546, B2650	MSNGM.230.407 and previous	MSNGM.230.408 and later
MS622	MSTGM.230.407 and previous	MSTGM.230.408 and later
M3250	MSTGM.230.407 and previous	MSTGM.230.408 and later
MX321	MXNGM.230.407 and previous	MXNGM.230.408 and later
MB2338	MXNGM.230.407 and previous	MXNGM.230.408 and later
MX421, MX521, MX522, MX622	MXTGM.230.407 and previous	MXTGM.230.408 and later
XM1242, XM1246, XM3250	MXTGM.230.407 and previous	MXTGM.230.408 and later
MB2442. MB2546, MB2650	MXTGM.230.407 and previous	MXTGM.230.408 and later
MS725, MS821, MS823, MS825	MSNGW.230.407 and previous	MSNGW.230.408 and later
B2865	MSNGW.230.407 and previous	MSNGW.230.408 and later
MS822, MS826	MSTGW.230.407 and previous	MSTGW.230.408 and later
M5255, M5270	MSTGW.230.407 and previous	MSTGW.230.408 and later

MX721, MX722, MX725, MX822, MX826	MXTGW.230.407 and previous	MXTGW.230.408 and later
XM5365, XM5370, XM7355, XM7370	MXTGW.230.407 and previous	MXTGW.230.408 and later
MB2770	MXTGW.230.407 and previous	MXTGW.230.408 and later
C3426	CSLBN.230.407 and previous	CSLBN.230.408 and later
CS431, CS439	CSLBN.230.407 and previous	CSLBN.230.408 and later
CS331	CSLBL.230.407 and previous	CSLBL.230.408 and later
C3224, C3326	CSLBL.230.407 and previous	CSLBL.230.408 and later
C2326	CSLBN.230.407 and previous	CSLBN.230.408 and later
MC3426	CXLBN.230.407 and previous	CXLBN.230.408 and later
CX431	CXLBN.230.407 and previous	CXLBN.230.408 and later
XC2326	CXLBN.230.407 and previous	CXLBN.230.408 and later
MC3426	CXLBN.230.407 and previous	CXLBN.230.408 and later
MC3224, MC3326	CXLBL.230.407 and previous	CXLBL.230.408 and later
CX331	CXLBL.230.407 and previous	CXLBL.230.408 and later
CS622	CSTZJ.230.407 and previous	CSTZJ.230.408 and later
C2240	CSTZJ.230.407 and previous	CSTZJ.230.408 and later
CS421, CS521	CSNZJ.230.407 and previous	CSNZJ.230.408 and later
C2325, C2425, C2535	CSNZJ.230.407 and previous	CSNZJ.230.408 and later
CX522, CX622, CX625	CXTZJ.230.407 and previous	CXTZJ.230.408 and later
XC2235, XC4240	CXTZJ.230.407 and previous	CXTZJ.230.408 and later
MC2535, MC2640	CXTZJ.230.407 and previous	CXTZJ.230.408 and later
CX421	CXNZJ.230.407 and previous	CXNZJ.230.408 and later
MC2325, MC2425	CXNZJ.230.407 and previous	CXNZJ.230.408 and later
CX820, CX825, CX827, CX860	CXTPP.230.407 and previous	CXTPP.230.408 and later
XC6152, XC6153, XC8155, XC8160, XC8163	CXTPP.230.407 and previous	CXTPP.230.408 and later
CS820, CS827	CSTPP.230.407 and previous	CSTPP.230.408 and later
C6160	CSTPP.230.407 and previous	CSTPP.230.408 and later
CS720, CS725, CS727, CS728	CSTAT.230.407 and previous	CSTAT.230.408 and later
C4150	CSTAT.230.407 and previous	CSTAT.230.408 and later
CX725, CX727	CXTAT.230.407 and previous	CXTAT.230.408 and later
XC4140, XC4143, XC4150, XC4153	CXTAT.230.407 and previous	CXTAT.230.408 and later
CS921, CS923, CS927	CSTMH.230.407 and previous	CSTMH.230.408 and later
C9235	CSTMH.230.407 and previous	CSTMH.230.408 and later
CX920, CX921, CX922, CX923, CX924	CXTMH.230.407 and previous	CXTMH.230.408 and later
XC9225, XC9235, XC9245, XC9255, XC9265	CXTMH.230.407 and previous	CXTMH.230.408 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

Setting an administrative password on the device (as prompted to do so during initial setup) will prevent an untrusted user from executing this vulnerability.

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:
DEVCORE Research Team

Status of this Notice:

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	18 November 2024	Initial Draft
0.2	17 January 2025	Updated firmware versions and publish date
1.0	30 January 2025	Public release version