Lexmark Security Advisory:

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

Summary

An integer overflow vulnerability has been identified in the Postscript interpreter in various Lexmark devices.

References

CVE: CVE-2024-11347

ZDI: ZDI-CAN-25676

CWE: CWE-190

Details

An integer overflow vulnerability has been identified in the Postscript interpreter in various Lexmark devices. The vulnerability can be leveraged by an attacker to execute arbitrary code as an unprivileged user.

CVSSv3 Base Score 7.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)
Impact Subscore: 3.4
Exploitability Subscore: 3.9

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 as an unprivileged user.

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.240.200	CXTLS.240.077 - CXTLS.240.199 CXTLS.240.201 and later
XC9525, XC9535	CXTLS.240.200	CXTLS.240.077 - CXTLS.240.199 CXTLS.240.201 and later
MX953	MXTLS.240.200	MXTLS.240.077 - MXTLS.240.199

		MXTLS.240.201 and later
CX961, CX962, CX963	CXTLS.240.076 and previous CXTLS.240.200	CXTLS.240.077 - CXTLS.240.199 CXTLS.240.201 and later
XC9635, XC9645, XC9655	CXTLS.240.076 and previous CXTLS.240.200	CXTLS.240.077 - CXTLS.240.199 CXTLS.240.201 and later
CS963	CSTLS.240.076 and previous CSTLS.240.200	CSTLS.240.077 - CSTLS.240.199 CSTLS.240.201 and later
CX833	CXTLS.240.076 and previous CXTLS.240.200	CXTLS.240.077 - CXTLS.240.199 CXTLS.240.201 and later
XC8355	CXTLS.240.076 and previous CXTLS.240.200	CXTLS.240.077 - CXTLS.240.199 CXTLS.240.201 and later
MS531, MS631	MSNSN.240.042 and previous MSNSN.240.200	MSNSN.240.043 - MSNSN.240.069 MSNSN.240.201 and later
MS632, M3350	MSTSN.240.042 and previous MSTSN.240.200	MSTSN.240.043 - MSTSN.240.069 MSTSN.240.201 and later
MX532, MX632, XM3350	MXTSN.240.042 and previous MXTSN.240.200	MXTSN.240.043 - MXTSN.240.069 MXTSN.240.201 and later
CS531, C2335	CSNGV.240.042 and previous CSNGV.240.200	CSNGV.240.043 - CSNGV.240.069 CSNGV.240.201 and later
CS632	CSTGV.240.042 and previous CSTGV.240.200	CSTGV.240.043 - CSTGV.240.069 CSTGV.240.201 and later
CX532, CX635, XC2335	CXTGV.240.042 and previous CXTGV.240.200	CXTGV.240.043 - CXTGV.240.069 CXTGV.240.201 and later
CX930, CX931, CX942, CX943, CX944	CXTPC.240.042 and previous CXTPC.240.200	CXTPC.240.043 - CXTPC.240.069 CXTPC.240.201 and later
XC9325, XC9335, XC9445, XC9455, XC9465	CXTPC.240.042 and previous CXTPC.240.200	CXTPC.240.043 - CXTPC.240.069 CXTPC.240.201 and later
CS943	CSTPC.240.042 and previous CSTPC.240.200	CSTPC.240.043 - CSTPC.240.069 CSTPC.240.201 and later
MX432	MXTCT.240.042 and previous MXTCT.240.200	MXTCT.240.043 - MXTCT.240.069 MXTCT.240.201 and later
XM3142	MXTCT.240.042 and previous MXTCT.240.200	MXTCT.240.043 - MXTCT.240.069 MXTCT.240.201 and later
MX931	MXTPM.240.042 and previous MXTPM.240.200	MXTPM.240.043-MXTPM.240.069 MXTPM.240.201 and later
CX730, CX735, CX737	CXTMM.240.042 and previous CXTMM.240.200	CXTMM.240.043-CXTMM.240.069 CXTMM.240.201 and later
XC4342, XC4352	CXTMM.240.042 and previous CXTMM.240.200	CXTMM.240.043-CXTMM.240.069 CXTMM.240.201 and later
CS730, CS735, CS737	CSTMM.240.042 and previous CSTMM.240.200	CSTMM.240.043 - CSTMM.240.069 CSTMM.240.201 and later
C4342, C4352	CSTMM.240.042 and previous CSTMM.240.200	CSTMM.240.043 - CSTMM.240.069 CSTMM.240.201 and later
B2236	MSLSG.230.401 and previous	MSLSG.230.402 and later
MB2236	MXLSG.230.401 and previous	MXLSG.230.402 and later
MS331, MS431, MS439	MSLBD.230.401 and previous	MSLBD.230.402 and later

M1342	MSLBD.230.401 and previous	MSLBD.230.402 and later
B3442, B3340	MSLBD.230.401 and previous	MSLBD.230.402 and later
XM1342	MXLBD.230.401 and previous	MXLBD.230.402 and later
MX331, MX431	MXLBD.230.401 and previous	MXLBD.230.402 and later
MB3442	MXLBD.230.401 and previous	MXLBD.230.402 and later
MS321, MS421, MS521, MS621	MSNGM.230.401 and previous	MSNGM.230.402 and later
M1242, M1246	MSNGM.230.401 and previous	MSNGM.230.402 and later
B2338, B2442, B2546, B2650	MSNGM.230.401 and previous	MSNGM.230.402 and later
MS622	MSTGM.230.401 and previous	MSTGM.230.402 and later
M3250	MSTGM.230.401 and previous	MSTGM.230.402 and later
MX321	MXNGM.230.401 and previous	MXNGM.230.402 and later
MB2338	MXNGM.230.401 and previous	MXNGM.230.402 and later
MX421, MX521, MX522, MX622	MXTGM.230.401 and previous	MXTGM.230.402 and later
XM1242, XM1246, XM3250	MXTGM.230.401 and previous	MXTGM.230.402 and later
MB2442. MB2546, MB2650	MXTGM.230.401 and previous	MXTGM.230.402 and later
MS725, MS821, MS823, MS825	MSNGW.230.401 and previous	MSNGW.230.402 and later
B2865	MSNGW.230.401 and previous	MSNGW.230.402 and later
MS822, MS826	MSTGW.230.401 and previous	MSTGW.230.402 and later
M5255, M5270	MSTGW.230.401 and previous	MSTGW.230.402 and later
MX721, MX722, MX725, MX822, MX826	MXTGW.230.401 and previous	MXTGW.230.402 and later
XM5365, XM5370, XM7355, XM7370	MXTGW.230.401 and previous	MXTGW.230.402 and later
MB2770	MXTGW.230.401 and previous	MXTGW.230.402 and later
C3426	CSLBN.230.401 and previous	CSLBN.230.402 and later
CS431, CS439	CSLBN.230.401 and previous	CSLBN.230.402 and later
CS331	CSLBL.230.401 and previous	CSLBL.230.402 and later
C3224, C3326	CSLBL.230.401 and previous	CSLBL.230.402 and later
C2326	CSLBN.230.401 and previous	CSLBN.230.402 and later
MC3426	CXLBN.230.401 and previous	CXLBN.230.402 and later
CX431	CXLBN.230.401 and previous	CXLBN.230.402 and later
XC2326	CXLBN.230.401 and previous	CXLBN.230.402 and later
MC3426	CXLBN.230.401 and previous	CXLBN.230.402 and later
MC3224, MC3326	CXLBL.230.401 and previous	CXLBL.230.402 and later
CX331	CXLBL.230.401 and previous	CXLBL.230.402 and later
CS622	CSTZJ.230.401 and previous	CSTZJ.230.402 and later
C2240	CSTZJ.230.401 and previous	CSTZJ.230.402 and later
CS421, CS521	CSNZJ.230.401 and previous	CSNZJ.230.402 and later
C2325, C2425, C2535	CSNZJ.230.401 and previous	CSNZJ.230.402 and later
CX522, CX622, CX625	CXTZJ.230.401 and previous	CXTZJ.230.402 and later
XC2235, XC4240	CXTZJ.230.401 and previous	CXTZJ.230.402 and later
MC2535, MC2640	CXTZJ.230.401 and previous	CXTZJ.230.402 and later
CX421	CXNZJ.230.401 and previous	CXNZJ.230.402 and later

MC2325, MC2425	CXNZJ.230.401 and previous	CXNZJ.230.402 and later
CX820, CX825, CX827, CX860	CXTPP.230.401 and previous	CXTPP.230.402 and later
XC6152, XC6153, XC8155, XC8160, XC8163	CXTPP.230.401 and previous	CXTPP.230.402 and later
CS820, CS827	CSTPP.230.401 and previous	CSTPP.230.402 and later
C6160	CSTPP.230.401 and previous	CSTPP.230.402 and later
CS720, CS725, CS727, CS728	CSTAT.230.401 and previous	CSTAT.230.402 and later
C4150	CSTAT.230.401 and previous	CSTAT.230.402 and later
CX725, CX727	CXTAT.230.401 and previous	CXTAT.230.402 and later
XC4140, XC4143, XC4150, XC4153	CXTAT.230.401 and previous	CXTAT.230.402 and later
CS921, CS923, CS927	CSTMH.230.401 and previous	CSTMH.230.402 and later
C9235	CSTMH.230.401 and previous	CSTMH.230.402 and later
CX920, CX921, CX922, CX923, CX924	CXTMH.230.401 and previous	CXTMH.230.402 and later
XC9225, XC9235, XC9245, XC9255, XC9265	CXTMH.230.401 and previous	CXTMH.230.402 and later
MS315, MS415, MS417	LW90.TL2.P215 and previous	LW90.TL2.P216 and later
MS510, MS517, MS610dn, MS617	LW90.PR2.P215 and previous	LW90.PR2.P216 and later
M1140+, M1145, M3150dn	LW90.PR2.P215 and previous	LW90.PR2.P216 and later
MS610de, M3150de	LW90.PR4.P215 and previous	LW90.PR4.P216 and later
MX410, MX417, MX510, MX511, MX517	LW90.SB4.P215 and previous	LW90.SB4.P216 and later
XM1140, XM1145	LW90.SB4.P215 and previous	LW90.SB4.P216 and later
MX610, MX611, MX617	LW90.SB7.P215 and previous	LW90.SB7.P216 and later
XM3150	LW90.SB7.P215 and previous	LW90.SB7.P216 and later
MS710, MS711, MS810dn, MS811, MS812dn, MS817, MS818	LW90.DN2.P215 and previous	LW90.DN2.P216 and later
M5163dn	LW90.DN2.P215 and previous	LW90.DN2.P216 and later
MS810de	LW90.DN4.P215 and previous	LW90.DN4.P216 and later
M5155, M5163de	LW90.DN4.P215 and previous	LW90.DN4.P216 and later
MS812de	LW90.DN7.P215 and previous	LW90.DN7.P216 and later
M5170	LW90.DN7.P215 and previous	LW90.DN7.P216 and later
MX710, MX711, MX717, MX718, MX810, MX811, MX812	LW90.TU.P215 and previous	LW90.TU.P216 and later
XM5163, XM5170, XM5263, XM5270, XM7155, XM7163, XM7170, XM7263, XM7270	LW90.TU.P215 and previous	LW90.TU.P216 and later
MS911	LW90.SA.P215 and previous	LW90.SA.P216 and later
MX910, MX911, MX912	LW90.MG.P215 and previous	LW90.MG.P216 and later
XM9145, XM9155, XM9165	LW90.MG.P215 and previous	LW90.MG.P216 and later
CX510, CX517	LW90.GM7.P215 and previous	LW90.GM7.P216 and later
XC2132	LW90.GM7.P215 and previous	LW90.GM7.P216 and later

XC2130	LW90.GM4.P215 and previous	LW90.GM4.P216 and later
CS510, CS517	LW90.VY4.P215 and previous	LW90.VY4.P216 and later
C2132	LW90.VY4.P215 and previous	LW90.VY4.P216 and later
CX410, CX417	LW90.GM4.P215 and previous	LW90.GM4.P216 and later
MS310, MS312, MS317, MS410	LW80.PRL.P257 and previous	LW80.PRL.P258 and later
M1140	LW80.PRL.P257 and previous	LW80.PRL.P258 and later
MX310, MX317	LW80.SB2.P257 and previous	LW80.SB2.P258 and later
XM1135	LW80.SB2.P257 and previous	LW80.SB2.P258 and later
CS310, CS317	LW80.VYL.P257 and previous	LW80.VYL.P258 and later
CS410, CS417	LW80.VY2.P257 and previous	LW80.VY2.P258 and later
CX310, CX317	LW80.GM2.P257 and previous	LW80.GM2.P258 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:
PHP Hooligans

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