Lexmark Security Advisory:

Revision:	1.1
Last update:	13 March 2023
Public Release Date:	10 March 2023

Summary

A vulnerability has been identified in the PostScript interpreter in various Lexmark devices.

References

CVE:	CVE-2023-26064
ZDI:	ZDI-CAN-19755
CWE:	CWE-847

Details

An out of bounds write vulnerability has been identified in PostScript interpreter in various Lexmark devices. The vulnerability can be leveraged by an attacker to execute arbitrary code.

CVSSv3 Base Score	9.0	(AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H)
Impact Subscore:	6.0	
Exploitability Subscore:	2.2	

CVSSv3 scores are calculated in accordance with CVSS version 3.1 (https://www.first.org/cvss/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 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**
CX930, CX931, CX942, CX943, CX944	CXTPC.081.231 and previous	CXTPC.081.232 and later
XC9325, XC9335, XC9445, XC9455, XC9465	CXTPC.081.231 and previous	CXTPC.081.232 and later
CS943	CSTPC.081.231 and previous	CSTPC.081.232 and later
MX432	MXTCT.081.231 and previous	MXTCT.081.232 and later
XM3142	MXTCT.081.231 and previous	MXTCT.081.232 and later
MX931	MXTPM.081.231 and previous	MXTPM.081.232 and later

CX730, CX735	CXTMM.081.231 and previous	CXTMM.081.232 and later
XC4342, XC4352	CXTMM.081.231 and previous	CXTMM.081.232 and later
CS730, CS735	CSTMM.081.231 and previous	CSTMM.081.232 and later
C4342, C4352	CSTMM.081.231 and previous	CSTMM.081.232 and later
B2236	MSLSG.081.231 and previous	MSLSG.081.232 and later
MB2236	MXLSG.081.231 and previous	MXLSG.081.232 and later
MS331, MS431, MS439	MSLBD.081.231 and previous	MSLBD.081.232 and later
M1342	MSLBD.081.231 and previous	MSLBD.081.232 and later
B3442, B3340	MSLBD.081.231 and previous	MSLBD.081.232 and later
XM1342	MXLBD.081.231 and previous	MXLBD.081.232 and later
MX331, MX431	MXLBD.081.231 and previous	MXLBD.081.232 and later
MB3442	MXLBD.081.231 and previous	MXLBD.081.232 and later
MS321, MS421, MS521, MS621	MSNGM.081.231 and previous	MSNGM.081.232 and later
M1242, M1246	MSNGM.081.231 and previous	MSNGM.081.232 and later
B2338, B2442, B2546, B2650	MSNGM.081.231 and previous	MSNGM.081.232 and later
MS622	MSTGM.081.231 and previous	MSTGM.081.232 and later
M3250	MSTGM.081.231 and previous	MSTGM.081.232 and later
MX321	MXNGM.081.231 and previous	MXNGM.081.232 and later
MB2338	MXNGM.081.231 and previous	MXNGM.081.232 and later
MX421, MX521, MX522, MX622	MXTGM.081.231 and previous	MXTGM.081.232 and later
XM1242, XM1246, XM3250	MXTGM.081.231 and previous	MXTGM.081.232 and later
MB2442. MB2546, MB2650	MXTGM.081.231 and previous	MXTGM.081.232 and later
MS725, MS821, MS823, MS825	MSNGW.081.231 and previous	MSNGW.081.232 and later
B2865	MSNGW.081.231 and previous	MSNGW.081.232 and later
MS822, MS826	MSTGW.081.231 and previous	MSTGW.081.232 and later
M5255, M5270	MSTGW.081.231 and previous	MSTGW.081.232 and later
MX721, MX722, MX725, MX822, MX826	MXTGW.081.231 and previous	MXTGW.081.232 and later
XM5365, XM5370, XM7355, XM7370	MXTGW.081.231 and previous	MXTGW.081.232 and later
MB2770	MXTGW.081.231 and previous	MXTGW.081.232 and later
C3426	CSLBN.081.231 and previous	CSLBN.081.232 and later
CS431, CS439	CSLBN.081.231 and previous	CSLBN.081.232 and later
CS331	CSLBL.081.231 and previous	CSLBL.081.232 and later
C3224, C3326	CSLBL.081.231 and previous	CSLBL.081.232 and later
C2326	CSLBN.081.231 and previous	CSLBN.081.232 and later
MC3426	CXLBN.081.231 and previous	CXLBN.081.232 and later
CX431	CXLBN.081.231 and previous	CXLBN.081.232 and later
XC2326	CXLBN.081.231 and previous	CXLBN.081.232 and later
MC3426	CXLBN.081.231 and previous	CXLBN.081.232 and later
MC3224, MC3326	CXLBL.081.231 and previous	CXLBL.081.232 and later
CX331	CXLBL.081.231 and previous	CXLBL.081.232 and later
CS622	CSTZJ.081.231 and previous	CSTZJ.081.232 and later
C2240	CSTZJ.081.231 and previous	CSTZJ.081.232 and later
CS421, CS521	CSNZJ.081.231 and previous	CSNZJ.081.232 and later

C2325, C2425, C2535	CSNZJ.081.231 and previous	CSNZJ.081.232 and later
CX522, CX622, CX625	CXTZJ.081.231 and previous	CXTZJ.081.232 and later
XC2235, XC4240	CXTZJ.081.231 and previous	CXTZJ.081.232 and later
MC2535, MC2640	CXTZJ.081.231 and previous	CXTZJ.081.232 and later
CX421	CXNZJ.081.231 and previous	CXNZJ.081.232 and later
MC2325, MC2425	CXNZJ.081.231 and previous	CXNZJ.081.232 and later
CX820, CX825, CX827, CX860	CXTPP.081.231 and previous	CXTPP.081.232 and later
XC6152, XC6153, XC8155, XC8160, XC8163	CXTPP.081.231 and previous	CXTPP.081.232 and later
CS820, CS827	CSTPP.081.231 and previous	CSTPP.081.232 and later
C6160	CSTPP.081.231 and previous	CSTPP.081.232 and later
CS720, CS725, CS727, CS728	CSTAT.081.231 and previous	CSTAT.081.232 and later
C4150	CSTAT.081.231 and previous	CSTAT.081.232 and later
CX725, CX727	CXTAT.081.231 and previous	CXTAT.081.232 and later
XC4140, XC4143, XC4150, XC4153	CXTAT.081.231 and previous	CXTAT.081.232 and later
CS921, CS923, CS927	CSTMH.081.231 and previous	CSTMH.081.232 and later
C9235	CSTMH.081.231 and previous	CSTMH.081.232 and later
CX920, CX921, CX922, CX923, CX924	CXTMH.081.231 and previous	CXTMH.081.232 and later
XC9225, XC9235, XC9245, XC9255, XC9265	CXTMH.081.231 and previous	CXTMH.081.232 and later
MS310, MS312, MS317, MS410	LW80.PRL.P233 and previous	LW80.PRL.P234 and later
M1140	LW80.PRL.P233 and previous	LW80.PRL.P234 and later
MS315, MS415, MS417	LW80.TL2.P233 and previous	LW80.TL2.P234 and later
MS510, MS517, MS610dn, MS617	LW80.PR2.P233 and previous	LW80.PR2.P234 and later
M1140+, M1145, M3150dn	LW80.PR2.P233 and previous	LW80.PR2.P234 and later
MS610de, M3150de	LW80.PR4.P233 and previous	LW80.PR4.P234 and later
MX310, MX317	LW80.SB2.P233 and previous	LW80.SB2.P234 and later
XM1135	LW80.SB2.P233 and previous	LW80.SB2.P234 and later
MX410, MX417, MX510, MX511, MX517	LW80.SB4.P233 and previous	LW80.SB4.P234 and later
XM1140, XM1145	LW80.SB4.P233 and previous	LW80.SB4.P234 and later
MX610, MX611, MX617	LW80.SB7.P233 and previous	LW80.SB7.P234 and later
XM3150	LW80.SB7.P233 and previous	LW80.SB7.P234 and later
MS710, MS711, MS810dn, MS811, MS812dn, MS817, MS818	LW80.DN2.P233 and previous	LW80.DN2.P234 and later
M5163dn	LW80.DN2.P233 and previous	LW80.DN2.P234 and later
MS810de	LW80.DN4.P233 and previous	LW80.DN4.P234 and later
M5155, M5163de	LW80.DN4.P233 and previous	LW80.DN4.P234 and later
MS812de	LW80.DN7.P233 and previous	LW80.DN7.P234 and later
M5170	LW80.DN7.P233 and previous	LW80.DN7.P234 and later
MX710, MX711, MX717, MX718, MX810, MX811, MX812	LW80.TU.P233 and previous	LW80.TU.P234 and later
XM5163, XM5170, XM5263,	LW80.TU.P233 and previous	LW80.TU.P234 and later

XM5270, XM7155, XM7163, XM7170, XM7263, XM7270		
MS911	LW80.SA.P233 and previous	LW80.SA.P234 and later
MX910, MX911, MX912	LW80.MG.P233 and previous	LW80.MG.P234 and later
XM9145, XM9155, XM9165	LW80.MG.P233 and previous	LW80.MG.P234 and later
MX6500e	LW80.JD.P233 and previous	LW80.JD.P234 and later
CS310, CS317	LW80.VYL.P233 and previous	LW80.VYL.P234 and later
CS410, CS417	LW80.VY2.P233 and previous	LW80.VY2.P234 and later
CS510, CS517	LW80.VY4.P233 and previous	LW80.VY4.P234 and later
C2132	LW80.VY4.P233 and previous	LW80.VY4.P234 and later
CX310, CX317	LW80.GM2.P233 and previous	LW80.GM2.P234 and later
CX410, CX417	LW80.GM4.P233 and previous	LW80.GM4.P234 and later
XC2130	LW80.GM4.P233 and previous	LW80.GM4.P234 and later
CX510, CX517	LW80.GM7.P233 and previous	LW80.GM7.P234 and later
XC2132	LW80.GM7.P233 and previous	LW80.GM7.P234 and later
C746	LHS60.CM2.P759 and previous	LHS60.CM2.P760 and later
C748, CS748	LHS60.CM4.P759 and previous	LHS60.CM4.P760 and later
C792, CS796	LHS60.HC.P759 and previous	LHS60.HC.P760 and later
C925	LHS60.HV.P759 and previous	LHS60.HV.P760 and later
C950	LHS60.TP.P759 and previous	LHS60.TP.P760 and later
X548, XS548	LHS60.VK.P759 and previous	LHS60.VK.P760 and later
X746, X748, XS748	LHS60.NY.P759 and previous	LHS60.NY.P760 and later
X792, XS795, XS796, XS798	LHS60.MR.P759 and previous	LHS60.MR.P760 and later
X925, XS925	LHS60.HK.P759 and previous	LHS60.HK.P760 and later
X950, X952, X954, XS950, XS955	LHS60.TQ.P759 and previous	LHS60.TQ.P760 and later
6500e	LHS60.JR.P759 and previous	LHS60.JR.P760 and later
C734	LR.SK.P837 and previous	LR.SK.P838 and later
C736	LR.SKE.P837 and previous	LR.SKE.P838 and later
E46x	LR.LBH.P837 and previous	LR.LBH.P838 and later
T65x	LR.JP.P837 and previous	LR.JP.P838 and later
X46x	LR.BS.P837 and previous	LR.BS.P838 and later
X65x	LR.MN.P837 and previous	LR.MN.P838 and later
X73x	LR.FL.P837 and previous	LR.FL.P838 and later
W850	LP.JB.P836 and previous	LP.JB.P837 and later
X86x	LP.SP.P836 and previous	LP.SP.P837 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:

Chris Anastasio

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
1.0	28 February 2023	Initial Public Release
1.1	13 March 2023	Updated Affected Products list