Lexmark Security Advisory:

Revision: 0.2
Last update: 6 February 2024
Public Release Date: 1 Apr 2024

Summary

A buffer overflow vulnerability has been identified in the Internet Printing Protocol (IPP) in various Lexmark devices.

References

CVE: CVE-2023-50739

ZDI: ZDI-CAN-22549

CWE: CWE-122

Details

A buffer overflow vulnerability has been identified in the Internet Printing Protocol (IPP) in various Lexmark devices. The vulnerability can be leveraged by an attacker to execute arbitrary code.

CVSSv3 Base Score	8.8	(AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Impact Subscore:	5.9	
Exploitability Subscore:	2.8	

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.230.209 and previous	CXTPC.230.210 and later
XC9325, XC9335, XC9445, XC9455, XC9465	CXTPC.230.209 and previous	CXTPC.230.210 and later
CS943	CSTPC.230.209 and previous	CSTPC.230.210 and later

MX432	MXTCT.230.209 and previous	MXTCT.230.210 and later
XM3142	MXTCT.230.209 and previous	MXTCT.230.210 and later
MX931	MXTPM.230.209 and previous	MXTPM.230.210 and later
CX730, CX735, CX737	CXTMM.230.209 and previous	CXTMM.230.210 and later
XC4342, XC4352	CXTMM.230.209 and previous	CXTMM.230.210 and later
CS730, CS735, CS737	CSTMM.230.209 and previous	CSTMM.230.210 and later
C4342, C4352	CSTMM.230.209 and previous	CSTMM.230.210 and later
B2236	MSLSG.230.209 and previous	MSLSG.230.210 and later
MB2236	MXLSG.230.209 and previous	MXLSG.230.210 and later
MS331, MS431, MS439	MSLBD.230.209 and previous	MSLBD.230.210 and later
M1342	MSLBD.230.209 and previous	MSLBD.230.210 and later
B3442, B3340	MSLBD.230.209 and previous	MSLBD.230.210 and later
XM1342	MXLBD.230.209 and previous	MXLBD.230.210 and later
MX331, MX431	MXLBD.230.209 and previous	MXLBD.230.210 and later
MB3442	MXLBD.230.209 and previous	MXLBD.230.210 and later
MS321, MS421, MS521, MS621	MSNGM.230.209 and previous	MSNGM.230.210 and later
M1242, M1246	MSNGM.230.209 and previous	MSNGM.230.210 and later
B2338, B2442, B2546, B2650	MSNGM.230.209 and previous	MSNGM.230.210 and later
MS622	MSTGM.230.209 and previous	MSTGM.230.210 and later
M3250	MSTGM.230.209 and previous	MSTGM.230.210 and later
MX321	MXNGM.230.209 and previous	MXNGM.230.210 and later
MB2338	MXNGM.230.209 and previous	MXNGM.230.210 and later
MX421, MX521, MX522, MX622	MXTGM.230.209 and previous	MXTGM.230.210 and later
XM1242, XM1246, XM3250	MXTGM.230.209 and previous	MXTGM.230.210 and later
MB2442. MB2546, MB2650	MXTGM.230.209 and previous	MXTGM.230.210 and later
MS725, MS821, MS823, MS825	MSNGW.230.209 and previous	MSNGW.230.210 and later
B2865	MSNGW.230.209 and previous	MSNGW.230.210 and later
MS822, MS826	MSTGW.230.209 and previous	MSTGW.230.210 and later
M5255, M5270	MSTGW.230.209 and previous	MSTGW.230.210 and later
MX721, MX722, MX725, MX822, MX826	MXTGW.230.209 and previous	MXTGW.230.210 and later
XM5365, XM5370, XM7355, XM7370	MXTGW.230.209 and previous	MXTGW.230.210 and later
MB2770	MXTGW.230.209 and previous	MXTGW.230.210 and later
C3426	CSLBN.230.209 and previous	CSLBN.230.210 and later
CS431, CS439	CSLBN.230.209 and previous	CSLBN.230.210 and later
CS331	CSLBL.230.209 and previous	CSLBL.230.210 and later
C3224, C3326	CSLBL.230.209 and previous	CSLBL.230.210 and later
C2326	CSLBN.230.209 and previous	CSLBN.230.210 and later
MC3426	CXLBN.230.209 and previous	CXLBN.230.210 and later
CX431	CXLBN.230.209 and previous	CXLBN.230.210 and later
XC2326	CXLBN.230.209 and previous	CXLBN.230.210 and later
MC3426	CXLBN.230.209 and previous	CXLBN.230.210 and later

MC3224, MC3326	CXLBL.230.209 and previous	CXLBL.230.210 and later
CX331	CXLBL.230.209 and previous	CXLBL.230.210 and later
CS622	CSTZJ.230.209 and previous	CSTZJ.230.210 and later
C2240	CSTZJ.230.209 and previous	CSTZJ.230.210 and later
CS421, CS521	CSNZJ.230.209 and previous	CSNZJ.230.210 and later
C2325, C2425, C2535	CSNZJ.230.209 and previous	CSNZJ.230.210 and later
CX522, CX622, CX625	CXTZJ.230.209 and previous	CXTZJ.230.210 and later
XC2235, XC4240	CXTZJ.230.209 and previous	CXTZJ.230.210 and later
MC2535, MC2640	CXTZJ.230.209 and previous	CXTZJ.230.210 and later
CX421	CXNZJ.230.209 and previous	CXNZJ.230.210 and later
MC2325, MC2425	CXNZJ.230.209 and previous	CXNZJ.230.210 and later
CX820, CX825, CX827, CX860	CXTPP.230.209 and previous	CXTPP.230.210 and later
XC6152, XC6153, XC8155, XC8160, XC8163	CXTPP.230.209 and previous	CXTPP.230.210 and later
CS820, CS827	CSTPP.230.209 and previous	CSTPP.230.210 and later
C6160	CSTPP.230.209 and previous	CSTPP.230.210 and later
CS720, CS725, CS727, CS728	CSTAT.230.209 and previous	CSTAT.230.210 and later
C4150	CSTAT.230.209 and previous	CSTAT.230.210 and later
CX725, CX727	CXTAT.230.209 and previous	CXTAT.230.210 and later
XC4140, XC4143, XC4150, XC4153	CXTAT.230.209 and previous	CXTAT.230.210 and later
CS921, CS923, CS927	CSTMH.230.209 and previous	CSTMH.230.210 and later
C9235	CSTMH.230.209 and previous	CSTMH.230.210 and later
CX920, CX921, CX922, CX923, CX924	CXTMH.230.209 and previous	CXTMH.230.210 and later
XC9225, XC9235, XC9245, XC9255, XC9265	CXTMH.230.209 and previous	CXTMH.230.210 and later
MS531, MS631	MSNSN.222.031 and previous MSNSN.230.001 thru MSNSN.230.209	MSNSN.222.032 thru MSNSN.222.999 MSNSN.230.210 and later
MS632, M3350	MSTSN.222.031 and previous MSTSN.230.001 thru MSTSN.230.209	MSTSN.222.032 thru MSTSN.222.999 MSTSN.230.210 and later
MX532, MX632, XM3350	MXTSN.222.031 and previous MXTSN.230.001 thru MXTSN.230.209	MXTSN.222.032 thru MXTSN.222.999 MXTSN.230.210 and later
CS531, C2335	CSNGV.222.031 and previous CSNGV.230.001 thru CSNGV.230.209	CSNGV.222.032 thru CSNGV.222.999 CSNGV.230.210 and later
CS632	CSTGV.222.031 and previous CSTGV.230.001 thru CSTGV.230.209	CSTGV.222.032 thru CSTGV.222.999 CSTGV.230.210 and later
CX532, CX635, XC2335	CXTGV.222.031 and previous CXTGV.230.001 thru CXTGV.230.209	CXTGV.222.032 thru CXTGV.222.999 CXTGV.230.210 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 Interrupt Labs working with Trend Micro's Zero Day Initiative (ZDI) for bringing this issue to our attention:

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	20 December 2023	Initial Draft
0.2	6 February 2024	Updated impacted versions