

Lexmark Security Advisory:

Revision: 1.0
Last update: 28 February 2023
Public Release Date: 10 March 2023

Summary

The embedded web server in newer Lexmark devices fails to properly sanitize input data which can lead to remote code execution on the device.

References

CVE: CVE-2023-26068

ZDI: ZDI-CAN-19766, ZDI-CAN-19774, ZDI-CAN-19470

CWE: CWE-20, CWE-267

Details

A vulnerability has been identified in the embedded web server used in Lexmark devices. The vulnerability allows the attacker to execute arbitrary code on a device with the permissions of the embedded webserver.

CVSSv3 Base Score 8.5 (AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H)
Impact Subscore: 6.0
Exploitability Subscore: 1.8

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.081.232 and previous	CXTPC.081.233 and later
XC9335, XC9445, XC9455, XC9465	CXTPC.081.232 and previous	CXTPC.081.233 and later
CS943	CSTPC.081.232 and previous	CSTPC.081.233 and later
MX432	MXTCT.081.232 and previous	MXTCT.081.233 and later
XM3142	MXTCT.081.232 and previous	MXTCT.081.233 and later

MX931	MXTPM.081.232 and previous	MXTPM.081.233 and later
CX730, CX735	CXTMM.081.232 and previous	CXTMM.081.233 and later
XC4342, XC4352	CXTMM.081.232 and previous	CXTMM.081.233 and later
CS730, CS735	CSTMM.081.232 and previous	CSTMM.081.233 and later
C4342, C4352	CSTMM.081.232 and previous	CSTMM.081.233 and later
B2236	MSLSG.081.232 and previous	MSLSG.081.233 and later
MB2236	MXLSG.081.232 and previous	MXLSG.081.233 and later
MS331, MS431	MSLBD.081.232 and previous	MSLBD.081.233 and later
M1342	MSLBD.081.232 and previous	MSLBD.081.233 and later
B3442, B3340	MSLBD.081.232 and previous	MSLBD.081.233 and later
XM1342	MSLBD.081.232 and previous	MSLBD.081.233 and later
MX331, MX431	MXLBD.081.232 and previous	MXLBD.081.233 and later
MB3442	MXLBD.081.232 and previous	MXLBD.081.233 and later
MS321, MS421, MS521, MS621	MSNGM.081.232 and previous	MSNGM.081.233 and later
M1242, M1246	MSNGM.081.232 and previous	MSNGM.081.233 and later
B2338, B2442, B2546, B2650	MSNGM.081.232 and previous	MSNGM.081.233 and later
MS622	MSTGM.081.232 and previous	MSTGM.081.233 and later
M3250	MSTGM.081.232 and previous	MSTGM.081.233 and later
MX321	MXNGM.081.232 and previous	MXNGM.081.233 and later
MB2338	MXNGM.081.232 and previous	MXNGM.081.233 and later
MX421, MX521, MX522, MX622	MXTGM.081.232 and previous	MXTGM.081.233 and later
XM1242, XM1246, XM3250	MXTGM.081.232 and previous	MXTGM.081.233 and later
MB2442, MB2546, MB2650	MXTGM.081.232 and previous	MXTGM.081.233 and later
MS725, MS821, MS823, MS825	MSNGW.081.232 and previous	MSNGW.081.233 and later
B2865	MSNGW.081.232 and previous	MSNGW.081.233 and later
MS822, MS826	MSTGW.081.232 and previous	MSTGW.081.233 and later
M5255, M5270	MSTGW.081.232 and previous	MSTGW.081.233 and later
MX721, MX722, MX822, MX826	MXTGW.081.232 and previous	MXTGW.081.233 and later
XM5365, XM7355, XM7370	MXTGW.081.232 and previous	MXTGW.081.233 and later
MB2770	MXTGW.081.232 and previous	MXTGW.081.233 and later
C3426	CSLBN.081.232 and previous	CSLBN.081.233 and later
CS431, CS439	CSLBN.081.232 and previous	CSLBN.081.233 and later
CS331	CSLBL.081.232 and previous	CSLBL.081.233 and later
C3224, C3326	CSLBL.081.232 and previous	CSLBL.081.233 and later
C2326	CSLBN.081.232 and previous	CSLBN.081.233 and later
MC3426	CXLBN.081.232 and previous	CXLBN.081.233 and later
CX431	CXLBN.081.232 and previous	CXLBN.081.233 and later
XC2326	CXLBN.081.232 and previous	CXLBN.081.233 and later
MC3426	CXLBN.081.232 and previous	CXLBN.081.233 and later
MC3224, MC3326	CXLBL.081.232 and previous	CXLBL.081.233 and later
CX331	CXLBL.081.232 and previous	CXLBL.081.233 and later
CS622	CSTZJ.081.232 and previous	CSTZJ.081.233 and later
C2240	CSTZJ.081.232 and previous	CSTZJ.081.233 and later
CS421, CS521	CSNZJ.081.232 and previous	CSNZJ.081.233 and later
C2325, C2425, C2535	CSNZJ.081.232 and previous	CSNZJ.081.233 and later
CX522, CX622, CX625	CXTZJ.081.232 and previous	CXTZJ.081.233 and later
XC2235, XC4240	CXTZJ.081.232 and previous	CXTZJ.081.233 and later

MC2535, MC2640	CXTZJ.081.232 and previous	CXTZJ.081.233 and later
CX421	CXNZJ.081.232 and previous	CXNZJ.081.233 and later
MC2325, MC2425	CXNZJ.081.232 and previous	CXNZJ.081.233 and later
CX820, CX825, CX827, CX860	CXTPP.081.232 and previous	CXTPP.081.233 and later
XC6152, XC6153, XC8155, XC8160, XC8163	CXTPP.081.232 and previous	CXTPP.081.233 and later
CS820, CS827	CSTPP.081.232 and previous	CSTPP.081.233 and later
C6160	CSTPP.081.232 and previous	CSTPP.081.233 and later
CS720, CS725, CS727, CS728	CSTAT.081.232 and previous	CSTAT.081.233 and later
C4150	CSTAT.081.232 and previous	CSTAT.081.233 and later
CX725, CX727	CXTAT.081.232 and previous	CXTAT.081.233 and later
XC4140, XC4143, XC4150, XC4153	CXTAT.081.232 and previous	CXTAT.081.233 and later
CS921, CS923, CS927	CSTMH.081.232 and previous	CSTMH.081.233 and later
C9235	CSTMH.081.232 and previous	CSTMH.081.233 and later
CX920, CX921, CX922, CX923, CX924	CXTMH.081.232 and previous	CXTMH.081.233 and later
XC9225, XC9235, XC9245, XC9255, XC9265	CXTMH.081.232 and previous	CXTMH.081.233 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:

James Horseman
Zach Hanley
Aleksei Stafeev
Pwn2Own Toronto 2022 DEVCOR team

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

<u>Revision</u>	<u>Date</u>	<u>Reason</u>
1.0	28 February 2023	Initial Public Release