Lexmark Security Advisory:

Revision:	1.2
Last update:	1 February 2021
Public Release Date:	3 February 2021

Summary

A vulnerability was found in the WiFi chip driver used in WiFi enabled Lexmark devices. Only devices with the WiFi feature installed and connected to a WiFi network are vulnerable.

References

CVE: CVE-2019-14816

Details

A vulnerability was found in the Linux kernel's Marvell WiFi chip driver. The vulnerability can be exploited by an attacker on the same WiFi physical network segment to cause a system crash resulting in a denial of service or potentially execution of arbitrary code.

CVSSv3 Base Score	7.8	(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Impact Subscore:	5.9	
Exploitability Subscore:	1.8	

CVSSv3 scores are calculated in accordance with CVSS version 3.1 (https://www.first.org/cvss/user-guide)

Impact

This vulnerability impacts devices with the WiFi feature installed and connected to a WiFi network. Successful exploitation of this vulnerability can lead to a system crash causing a denial of service or execution of arbitrary code.

Affected Products

To determine a device’s 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
B2236	MSLSG.073.023 and previous	MSLSG.073.225 and later
MS331, MS431	MSLBD.073.023 and previous	MSLBD.073.225 and later
M1241	MSLBD.073.023 and previous	MSLBD.073.225 and later
B3442, B3340	MSLBD.073.023 and previous	MSLBD.073.225 and later

MB2236	MXLSG.073.023 and previous	MXLSG.073.225 and later
MX431, MX331	MXLBD.073.023 and previous	MXLBD.073.225 and later
MB3442	MXLBD.073.023 and previous	MXLBD.073.225 and later
MS521	MSNGM.073.023 and previous	MSNGM.073.225 and later
MS621, MS622	MSTGM.073.023 and previous	MSTGM.073.225 and later
M1246, M3250	MSTGM.073.023 and previous	MSTGM.073.225 and later
B2546, B2650	MSTGM.073.023 and previous	MSTGM.073.225 and later
MX421, MX521, MX522, MX622	MXTGM.073.023 and previous	MXTGM.073.225 and later
XM1242, XM1246, XM3250	MXTGM.073.023 and previous	MXTGM.073.225 and later
MB2546, MB2650	MXTGM.073.023 and previous	MXTGM.073.225 and later
MX321	MXNGM.073.023 and previous	MXNGM.073.225 and later
MB2338	MXNGM.073.023 and previous	MXNGM.073.225 and later
MS725, MS821	MSNGW.073.023 and previous	MSNGW.073.225 and later
MS822, MS823, MS825, MS826	MSTGW.073.023 and previous	MSTGW.073.225 and later
M5255, M5270	MSTGW.073.023 and previous	MSTGW.073.225 and later
B2865	MSTGW.073.023 and previous	MSTGW.073.225 and later
MX721, MX722, MX822, MX826	MXTGW.073.023 and previous	MXTGW.073.225 and later
XM5365, XM7355, XM7370	MXTGW.073.023 and previous	MXTGW.073.225 and later
C3426	CSLBN.073.023 and previous	CSLBN.073.225 and later
CS431	CSLBN.073.023 and previous	CSLBN.073.225 and later
CS331	CSLBL.073.023 and previous	CSLBL.073.225 and later
C3224	CSLBL.073.023 and previous	CSLBL.073.225 and later
C3326	CSLBL.073.023 and previous	CSLBL.073.225 and later
MC3426	CXLBN.073.023 and previous	CXLBN.073.225 and later
CX431	CXLBN.073.023 and previous	CXLBN.073.225 and later
MC3326, MC3224	CXLBL.073.023 and previous	CXLBL.073.225 and later
CX331	CXLBL.073.023 and previous	CXLBL.073.225 and later
CS622	CSTZJ.073.023 and previous	CSTZJ.073.225 and later
C2240	CSTZJ.073.023 and previous	CSTZJ.073.225 and later
CS421, CS521	CSNZJ.073.023 and previous	CSNZJ.073.225 and later
C2535, C2325, C2425	CSNZJ.073.023 and previous	CSNZJ.073.225 and later
CX522, CX622, CX625	CXTZJ.073.023 and previous	CXTZJ.073.225 and later
XC2235, XC4240	CXTZJ.073.023 and previous	CXTZJ.073.225 and later
MC2535, MC2640	CXTZJ.073.023 and previous	CXTZJ.073.225 and later
CX421	CXNZJ.073.023 and previous	CXNZJ.073.225 and later
MC2325, MC2425	CXNZJ.073.023 and previous	CXNZJ.073.225 and later

CX820, CX825, CX860	CXTPP.073.023 and previous	CXTPP.073.225 and later
XC6152, XC8155, XC8160	CXTPP.073.023 and previous	CXTPP.073.225 and later
CS820	CSTPP.073.023 and previous	CSTPP.073.225 and later
C6160	CSTPP.073.023 and previous	CSTPP.073.225 and later
CS720, CS725	CSTAT.073.023 and previous	CSTAT.073.225 and later
C4150	CSTAT.073.023 and previous	CSTAT.073.225 and later
CX725	CXTAT.073.023 and previous	CXTAT.073.225 and later
XC4140, XC4150	CXTAT.073.023 and previous	CXTAT.073.225 and later
CS921, CS923	CSTMH.073.023 and previous	CSTMH.073.225 and later
CX921, CX922, CX923, CX924	CXTMH.073.023 and previous	CXTMH.073.225 and later
XC92xx	CXTMH.073.023 and previous	CXTMH.073.225 and later

Obtained 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. If you can not update your firmware, you can also workaround this vulnerability by removing the wireless card from your printer or disabling wireless on your device.

Exploitation and Public Announcements

Lexmark is not aware of any malicious use against Lexmark products of the vulnerability described in this advisory.

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.

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
1.1	12 October 2020	Initial Public Release
1.2	1 February 2021	Additional clarification of scope