Lexmark Security Advisory:

Revision: 1.3
Last update: 14 September 2018
Public Release Date: 27 August 2018

Summary

Lexmark has identified a buffer overflow vulnerability in some models of multi-function devices handling of color fax jobs.

This issue is not related to CVE-2018-5925 and CVE-2018-5924.

References

CVE: CVE-2018-15519, CVE-2018-15520

Details

CVE-2018-15519

This vulnerability allows an attacker with crafted fax data to attack a Lexmark multifunction device. The vulnerability allows a remote attacker to execute arbitrary code via crafted color fax data.

CVSS v3 Base Score:	9.8	(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Impact Subscore:	5.9	
Exploitability Score:	3.9	

CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss/user-guide)

CVE-2018-15520

This vulnerability allows an attacker with crafted fax data to attack a Lexmark multifunction device. This vulnerability allows a remote attacker to crash the device, creating a denial of service condition, or possibly to have unspecified other impact via crafted color fax data.

CVSS v3 Base Score:	7.5	(AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
Impact Score:	3.6	
Exploitability Score:	3.9	

CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss/user-guide)

Impact

CVE-2018-15519

Successful exploitation of this vulnerability can also lead to an attacker being able to remotely execute arbitrary code on a device. This condition may continue until the crafted fax data is wiped from the device.
For instructions on recovering a device in this state, contact the Lexmark Technical Support Center.

CVE-2018-15520
Successful exploitation of this vulnerability can lead to an attacker being able to crash a device, resulting in a denial-of-service until the crafted fax data is wiped from the device.
For instructions on recovering a device in this state, contact the Lexmark Technical Support Center.

Affected Products

Many Lexmark products support Fax, and are affected by this vulnerability when they receive and process color fax jobs. The complete list of affected devices is shown below.

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 you should upgrade to a "**Fixed Release**".

CVE-2018-15519

Lexmark Models	**Affected Releases**	**Fixed Releases**
CX310	LW70.GM2.P204 and previous	LW70.GM2.P205 and later
CX410	LW70.GM4.P204 and previous	LW70.GM4.P205 and later
CX510, XC2132	LW70.GM7.P204 and previous	LW70.GM7.P205 and later
MX31x	LW70.SB2.P204 and previous	LW70.SB2.P205 and later
MX41x, MX51x, XM1145	LW70.SB4.P204 and previous	LW70.SB4.P205 and later
MX61x, XM3150	LW70.SB7.P204 and previous	LW70.SB7.P205 and later
MX71x, MX81x, XM51xx, XM71xx	LW70.TU.P204 and previous	LW70.TU.P205 and later
MX91x, XM91x	LW70.MG.P204 and previous	LW70.MG.P205 and later
MX6500	LW70.JD.P204 and previous	LW70.JD.P205 and later
X54x, XS54x	LHS60.VK.P671 and previous	LHS60.VK.P672 and later
X74x, XS74x	LHS60.NY.P671 and previous	LHS60.NY.P672 and later
X79x, XS79x	LHS60.MR.P671 and previous	LHS60.MR.P672 and later
X92x, XS92x	LHS60.HK.P671 and previous	LHS60.HK.P672 and later
X95x, XS95x	LHS60.TQ.P671 and previous	LHS60.TQ.P672 and later
6500	LHS60.JR.P671 and previous	LHS60.JR.P672 and later
X46x	LR.BS.P803 and previous	LR.BS.P804 and later
X65x	LR.MN.P803 and previous	LR.MN.P804 and later
X73x	LR.FL.P803 and previous	LR.FL.P804 and later
X86x	LP.SP.P803 and previous	LP.SP.P804 and later

CVE-2018-15520

Lexmark Models	Affected Releases	Fixed Releases
CX82x, CX860, XC6152, XC8155, XC8160	CXTPP.052.024 and previous, plus 052.200 through 052.204	CXTPP.052.025 and later, excluding 052.200 through 052.204
CX72x, XC41x0	CXTAT.052.024 and previous, plus 052.200 through 052.204	CXTAT.052.025 and later, excluding 052.200 through 052.204
CX92x, XC92x5	CXTMH.052.024 and previous, plus 052.200 through 052.204	CXTMH.052.025 and later, excluding 052.200 through 052.204
MX321, MB2338	MXNGM.052.024 and previous, plus 052.200 through 052.204	MXNGM.052.025 and later, excluding 052.200 through 052.204
MX42x, MX52x, MX622, MB2442, MB2546, MB2650, XM124x, XM3250	MXTGM.052.024 and previous, plus 052.200 through 052.204	MXTGM.052.025 and later, excluding 052.200 through 052.204
MX72x, MX82x, MB2770, XM5370, XM7355, XM7370	MXTGW.052.024 and previous, plus 052.200 through 052.204	MXTGW.052.025 and later, excluding 052.200 through 052.204
CX421, MC2325, MC2425	CXNZJ.052.024 and previous, plus 052.200 through 052.204	CXNZJ.052.025 and later, excluding 052.200 through 052.204
CX522, CX62x, MC2535, MC2640, XC2235, XC4240	CXTZJ.052.024 and previous, plus 052.200 through 052.204	CXTZJ.052.025 and later, excluding 052.200 through 052.204

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

Disabling the “Enable Color Fax Receive” feature on a device will block the ability to exploit this vulnerability.

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
1.0	27 - August 2018	Initial Public Release
1.1	28 - August 2018	Update list of affected models
1.2	29 - August 2018	Update list of affected models
1.3	14 - September 2018	Update to vector values for CVE-2018-15519