Lexmark Security Advisory:

Revision: 1.0
Last update: 11 February 2019
Public Release Date: 11 February 2019

Summary

Many older Lexmark devices contain a vulnerability that allows an unauthenticated user to purge stored shortcuts.

References

CVE: CVE-2019-6489

Details

A vulnerability has been identified in the embedded web server used in older generation Lexmark devices. The vulnerability allows an unauthenticated user to purge/erase shortcuts stored on the device.

CVSSv3 Base Score	6.5	(AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L)
Impact Subscore:	2.5	
Exploitability Subscore:	3.9	

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

Impact

Successful exploitation of this vulnerability can lead to the erasure of stored shortcuts on the affected device.

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**
CX310	LW71.GM2.P216 and previous	LW71.GM2.P217 and later
CX410 & XC2130	LW71.GM4.P216 and previous	LW71.GM4.P217 and later
CX510 & XC2132	LW71.GM7.P216 and previous	LW71.GM7.P217 and later
MX31x & XM1135	LW71.SB2.P216 and previous	LW71.SB2.P217 and later
MX410, MX510 & MX511	LW71.SB4.P216 and previous	LW71.SB4.P217 and later
XM1140 & XM1145	LW71.SB4.P216 and previous	LW71.SB4.P217 and later

MX610 & MX611	LW71.SB7.P216 and previous	LW71.SB7.P217 and later
XM3150	LW71.SB7.P216 and previous	LW71.SB7.P217 and later
MX71x	LW71.TU.P216 and previous	LW71.TU.P217 and later
MX81x	LW71.TU.P216 and previous	LW71.TU.P217 and later
XM51xx & XM71xx	LW71.TU.P216 and previous	LW71.TU.P217 and later
MX91x & XM91x	LW71.MG.P216 and previous	LW71.MG.P217 and later
MX6500e	LW71.JD.P216 and previous	LW71.JD.P217 and later
X548 & XS548	LHS60.VK.P682 and previous	LHS60.VK.P683 and later
X74x & XS748	LHS60.NY.P682 and previous	LHS60.NY.P683 and later
X792 & XS79x	LHS60.MR.P682 and previous	LHS60.MR.P683 and later
X925 & XS925	LHS60.HK.P682 and previous	LHS60.HK.P683 and later
X95x & XS95x	LHS60.TQ.P682 and previous	LHS60.TQ.P683 and later
6500e	LHS60.JR.P809 and previous	LHS60.JR.P810 and later
X46x	LR.BS.P809 and previous	LR.BS.P810 and later
X65x	LR.MN.P809 and previous	LR.MN.P810 and later
X73x	LR.FL.P809 and previous	LR.FL.P810 and later
X86x	LP.SP.P809 and previous	LP.SP.P810 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 Matthew Lichtenberger of Apple for bringing this 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
1.0	11 February 2019	Initial Public Release