Lexmark Security Advisory:

Revision: 1.1
Last update: 25-Feb-2021
Public Release Date: 18-Dec-2018

Summary

Lexmark devices contain a directory traversal vulnerability.
This advisory has been updated to list additional affected devices listed in **bold.**

References

CVE: CVE-2018-18894

Details

A directory traversal vulnerability has been identified in the embedded web server used in older generation Lexmark devices. The vulnerability allows unauthenticated access to sensitive files on the device.

CVSSv3 Base Score	7.5	(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Impact Subscore:	3.6	
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 disclosure of configuration and operating system information 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**
CX82x, CX860, XC6152, XC8155, XC8160	**CXTPP.041.243 and previous**	**CXTPP.050.040 and later**
CX72x, XC41x0	**CXTAT.041.243 and previous**	**CXTAT.050.040 and later**
CX92x, XC92x5	**CXTMH.041.243 and previous**	**CXTMH.050.040 and later**
CS820, C6160	**CSTPP.041.243 and previous**	**CSTPP.050.040 and later**
CS72x, C4150	**CSTAT.041.243 and previous**	**CSTAT.050.040 and later**
CS92x	**CSTMH.041.243 and previous**	**CSTMH.050.040 and later**

CS41x	LW71.VY2.P215 and previous	LW71.VY2.P216 and later
CS51x	LW71.VY4.P215 and previous	LW71.VY4.P216 and later
CX410	LW71.GM4.P215 and previous	LW71.GM4.P216 and later
CX510 & XC2132	LW71.GM7.P215 and previous	LW71.GM7.P216 and later
MS610de & MS610dte	LW71.PR4.P215 and previous	LW71.PR4.P216 and later
M3150	LW71.PR4.P215 and previous	LW71.PR4.P216 and later
MS810de	LW71.DN4.P215 and previous	LW71.DN4.P216 and later
M5155 & M5163	LW71.DN4.P215 and previous	LW71.DN4.P216 and later
MS812de	LW71.DN7.P215 and previous	LW71.DN7.P216 and later
M5170	LW71.DN7.P215 and previous	LW71.DN7.P216 and later
MS91x	LW71.SA.P215 and previous	LW71.SA.P216 and later
MX410, MX510 & MX511	LW71.SB4.P215 and previous	LW71.SB4.P216 and later
XM1145	LW71.SB4.P215 and previous	LW71.SB4.P216 and later
MX610 & MX611	LW71.SB7.P215 and previous	LW71.SB7.P216 and later
XM3150	LW71.SB7.P215 and previous	LW71.SB7.P216 and later
MX71x	LW71.TU.P215 and previous	LW71.TU.P216 and later
MX81x	LW71.TU.P215 and previous	LW71.TU.P216 and later
XM51xx & XM71xx	LW71.TU.P215 and previous	LW71.TU.P216 and later
MX91x & XM91x	LW71.MG.P215 and previous	LW71.MG.P216 and later
MX6500e	LW71.JD.P215 and previous	LW71.JD.P216 and later
C748 & CS748	LHS60.CM4.P682 and previous	LHS60.CM4.P683 and later
C79x & CS796	LHS60.HC.P682 and previous	LHS60.HC.P683 and later
C925	LHS60.HV.P682 and previous	LHS60.HV.P683 and later
C95x	LHS60.TP.P682 and previous	LHS60.TP.P683 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.P682 and previous	LHS60.JR.P683 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
C734	**LR.SK.P809 and previous**	**LR.SK.P810 and later**
W850	**LR.JB.P809 and previous**	**LR.JB.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 Benjamin Rollin of GuidePoint Security 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	18 December 2018	Initial Public Release
1.1	25 February 2021	Updated affected product List