

Lexmark Security Advisory:

Revision: 1.0
Last update: 10-May-2019
Public Release Date: 20-May-2019

Summary

Many older Lexmark devices embedded web server contain a cross site request forgery attack vulnerability that allows a local account password to be changed without the knowledge of the authenticated user.

References

CVE: CVE-2019-10057

Details

A vulnerability has been identified in the embedded web server used in older generation Lexmark devices. The vulnerability allows an attacker to fool an authenticated user into changing their password.

CVSSv3 Base Score 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N)
Impact Subscore: 3.6
Exploitability Subscore: 2.8

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 takeover of a local account on the 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
CS31x	LW71.VYL.P228 and previous	LW71.VYL.P229 and later
CS41x	LW71.VY2.P228 and previous	LW71.VY2.P229 and later
CX310	LW71.GM2.P228 and previous	LW71.GM2.P229 and later
MS310, MS312, MS317	LW71.PRL.P228 and previous	LW71.PRL.P229 and later
MS410, M1140	LW71.PRL.P228 and previous	LW71.PRL.P229 and later
MS315, MS415, MS417	LW71.TL2.P228 and previous	LW71.TL2.P229 and later
MX31x, XM1135	LW71.SB2.P228 and previous	LW71.SB2.P229 and later
MS51x, MS610dn, MS617	LW71.PR2.P228 and previous	LW71.PR2.P229 and later
M1145, M3150dn	LW71.PR2.P228 and previous	LW71.PR2.P229 and later
MS71x, M5163dn	LW71.DN2.P228 and previous	LW71.DN2.P229 and later

MS810, MS811, MS812, MS817, MS818	LW71.DN2.P228 and previous	LW71.DN2.P229 and later
CS51x	LW63.VY4.P683 and previous	LW63.VY4.P684 and later
CX410 & XC2130	LW63.GM4.P683 and previous	LW63.GM4.P684 and later
CX510 & XC2132	LW63.GM7.P683 and previous	LW63.GM7.P684 and later
MS610de, M3150	LW63.PR4.P683 and previous	LW63.PR4.P684 and later
MS810de, M5155, M5163	LW63.DN4.P683 and previous	LW63.DN4.P684 and later
MS812de, M5170	LW63.DN7.P683 and previous	LW63.DN7.P684 and later
MS91x	LW63.SA.P683 and previous	LW63.SA.P684 and later
MX31x, XM1135	LW63.SB2.P683 and previous	LW63.SB2.P684 and later
MX410, MX510 & MX511	LW63.SB4.P683 and previous	LW63.SB4.P684 and later
XM1140, XM1145	LW63.SB4.P683 and previous	LW63.SB4.P684 and later
MX610 & MX611	LW63.SB7.P683 and previous	LW63.SB7.P684 and later
XM3150	LW63.SB7.P683 and previous	LW63.SB7.P684 and later
MX71x, MX81x	LW63.TU.P683 and previous	LW63.TU.P684 and later
XM51xx & XM71xx	LW63.TU.P683 and previous	LW63.TU.P684 and later
MX91x & XM91x	LW63.MG.P683 and previous	LW63.MG.P684 and later
MX6500e	LW63.JD.P683 and previous	LW63.JD.P684 and later
C746	LHS42.CM2.P573 and previous	LHS42.CM2.P574 and later
C748, CS748	LHS42.CM4.P573 and previous	LHS42.CM4.P574 and later
C792, CS796	LHS42.HC.P573 and previous	LHS42.HC.P574 and later
C925	LHS42.HV.P573 and previous	LHS42.HV.P574 and later
C950	LHS42.TP.P573 and previous	LHS42.TP.P574 and later
X548 & XS548	LHS42.VK.P573 and previous	LHS42.VK.P574 and later
X74x & XS748	LHS42.NY.P573 and previous	LHS42.NY.P574 and later
X792 & XS79x	LHS42.MR.P573 and previous	LHS42.MR.P574 and later
X925 & XS925	LHS42.HK.P573 and previous	LHS42.HK.P574 and later
X95x & XS95x	LHS42.TQ.P573 and previous	LHS42.TQ.P574 and later
6500e	LHS42.JR.P573 and previous	LHS42.JR.P574 and later
C734	LR.SK.P743 and previous	LR.SK.P744 and later
C736	LR.SKE.P743 and previous	LR.SKE.P744 and later
E46x	LR.LBH.P743 and previous	LR.LBH.P744 and later
T65x	LR.JP.P743 and previous	LR.JP.P744 and later
X46x	LR.BS.P743 and previous	LR.BS.P744 and later
X65x	LR.MN.P743 and previous	LR.MN.P744 and later
X73x	LR.FL.P743 and previous	LR.FL.P744 and later
W850	LP.JB.P742 and previous	LP.JB.P743 and later
X86x	LP.SP.P742 and previous	LP.SP.P743 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 Daniel Romero and Mario Rivas of NCC group for bringing this issue 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

<u>Revision</u>	<u>Date</u>	<u>Reason</u>
1.0	20-May-2019	Initial Public Release