Lexmark Security Advisory:

Revision: 1.1
Last update: 22 June 2020
Public Release Date: 26 June 2020

Summary

A stored cross site scripting vulnerability has been identified in Lexmark devices.

References

CVE: CVE-2020-13481

Details

A stored cross site scripting vulnerability has been identified in the embedded web server used in Lexmark devices. The vulnerability can be used to attack the user's browser, exposing session credentials and other information accessible to the browser.

CVSSv3 Base Score   5.7   (AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N)
Impact Subscore: 3.6
Exploitability Subscore: 2.1

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

Impact

Successful exploitation of this vulnerability can lead to disclosure of information accessible to the browser.

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
B2236	MSLSG.073.022 – 073.023 AND 072.209 and previous	MSLSG.072.210 – 072.224 AND 073.225 and later
MS331, MS431	MSLBD.073.022 – 073.023 AND 072.209 and previous	MSLBD.072.210 – 072.224 AND 073.225 and later
M1241	MSLBD.073.022 – 073.023 AND 072.209 and previous	MSLBD.072.210 – 072.224 AND 073.225 and later
B3442, B3340	MSLBD.073.022 – 073.023 AND 072.209 and previous	MSLBD.072.210 – 072.224 AND 073.225 and later
MB2236	MXLSG.073.022 – 073.023 AND 072.209 and previous	MXLSG.072.210 – 072.224 AND 073.225 and later
MX431, MX331	MXLBD.073.022 – 073.023 AND 072.209 and previous	MXLBD.072.210 – 072.224 AND 073.225 and later
MB3442	MXLBD.073.022 – 073.023	MXLBD.072.210 – 072.224 AND

	AND 072.209 and previous	073.225 and later
MS521	MSNGM.073.022 – 073.023 AND 072.209 and previous	MSNGM.072.210 – 072.224 AND 073.225 and later
MS621, MS622	MSTGM.073.022 – 073.023 AND 072.209 and previous	MSTGM.072.210 – 072.224 AND 073.225 and later
M1246, M3250	MSTGM.073.022 – 073.023 AND 072.209 and previous	MSTGM.072.210 – 072.224 AND 073.225 and later
B2546, B2650	MSTGM.073.022 – 073.023 AND 072.209 and previous	MSTGM.072.210 – 072.224 AND 073.225 and later
MX421, MX521, MX522, MX622	MXTGM.073.022 – 073.023 AND 072.209 and previous	MXTGM.072.210 – 072.224 AND 073.225 and later
XM1242, XM1246, XM3250	MXTGM.073.022 – 073.023 AND 072.209 and previous	MXTGM.072.210 – 072.224 AND 073.225 and later
MB2546, MB2650	MXTGM.073.022 – 073.023 AND 072.209 and previous	MXTGM.072.210 – 072.224 AND 073.225 and later
MX321	MXNGM.073.022 – 073.023 AND 072.209 and previous	MXNGM.072.210 – 072.224 AND 073.225 and later
MB2338	MXNGM.073.022 – 073.023 AND 072.209 and previous	MXNGM.072.210 – 072.224 AND 073.225 and later
MS725, MS821	MSNGW.073.022 – 073.023 AND 072.209 and previous	MSNGW.072.210 – 072.224 AND 073.225 and later
MS822, MS823, MS825, MS826	MSTGW.073.022 – 073.023 AND 072.209 and previous	MSTGW.072.210 – 072.224 AND 073.225 and later
M5255, M5270	MSTGW.073.022 – 073.023 AND 072.209 and previous	MSTGW.072.210 – 072.224 AND 073.225 and later
B2865	MSTGW.073.022 – 073.023 AND 072.209 and previous	MSTGW.072.210 – 072.224 AND 073.225 and later
MX721, MX722, MX822, MX826	MXTGW.073.022 – 073.023 AND 072.209 and previous	MXTGW.072.210 – 072.224 AND 073.225 and later
XM5365, XM7355, XM7370	MXTGW.073.022 – 073.023 AND 072.209 and previous	MXTGW.072.210 – 072.224 AND 073.225 and later
C3426	CSLBN.073.022 – 073.023 AND 072.209 and previous	CSLBN.072.210 – 072.224 AND 073.225 and later
CS431	CSLBN.073.022 – 073.023 AND 072.209 and previous	CSLBN.072.210 – 072.224 AND 073.225 and later
CS331	CSLBL.073.022 – 073.023 AND 072.209 and previous	CSLBL.072.210 – 072.224 AND 073.225 and later
C3224	CSLBL.073.022 – 073.023 AND 072.209 and previous	CSLBL.072.210 – 072.224 AND 073.225 and later
C3326	CSLBL.073.022 – 073.023 AND 072.209 and previous	CSLBL.072.210 – 072.224 AND 073.225 and later
MC3426	CXLBN.073.022 – 073.023 AND 072.209 and previous	CXLBN.072.210 – 072.224 AND 073.225 and later
CX431	CXLBN.073.022 – 073.023 AND 072.209 and previous	CXLBN.072.210 – 072.224 AND 073.225 and later
MC3326, MC3224	CXLBL.073.022 – 073.023 AND 072.209 and previous	CXLBL.072.210 – 072.224 AND 073.225 and later
CX331	CXLBL.073.022 – 073.023 AND 072.209 and previous	CXLBL.072.210 – 072.224 AND 073.225 and later
CS622	CSTZJ.073.022 – 073.023 AND 072.209 and previous	CSTZJ.072.210 – 072.224 AND 073.225 and later

C2240	CSTZJ.073.022 – 073.023 AND 072.209 and previous	CSTZJ.072.210 – 072.224 AND 073.225 and later
CS421, CS521	CSNZJ.073.022 – 073.023 AND 072.209 and previous	CSNZJ.072.210 – 072.224 AND 073.225 and later
C2535, C2325, C2425	CSNZJ.073.022 – 073.023 AND 072.209 and previous	CSNZJ.072.210 – 072.224 AND 073.225 and later
CX522, CX622, CX625	CXTZJ.073.022 – 073.023 AND 072.209 and previous	CXTZJ.072.210 – 072.224 AND 073.225 and later
XC2235, XC4240	CXTZJ.073.022 – 073.023 AND 072.209 and previous	CXTZJ.072.210 – 072.224 AND 073.225 and later
MC2535, MC2640	CXTZJ.073.022 – 073.023 AND 072.209 and previous	CXTZJ.072.210 – 072.224 AND 073.225 and later
CX421	CXNZJ.073.022 – 073.023 AND 072.209 and previous	CXNZJ.072.210 – 072.224 AND 073.225 and later
MC2325, MC2425	CXNZJ.073.022 – 073.023 AND 072.209 and previous	CXNZJ.072.210 – 072.224 AND 073.225 and later
CX820, CX825, CX860	CXTPP.073.022 – 073.023 AND 072.209 and previous	CXTPP.072.210 – 072.224 AND 073.225 and later
XC6152, XC8155, XC8160	CXTPP.073.022 – 073.023 AND 072.209 and previous	CXTPP.072.210 – 072.224 AND 073.225 and later
CS820	CSTPP.073.022 – 073.023 AND 072.209 and previous	CSTPP.072.210 – 072.224 AND 073.225 and later
C6160	CSTPP.073.022 – 073.023 AND 072.209 and previous	CSTPP.072.210 – 072.224 AND 073.225 and later
CS720, CS725	CSTAT.073.022 – 073.023 AND 072.209 and previous	CSTAT.072.210 – 072.224 AND 073.225 and later
C4150	CSTAT.073.022 – 073.023 AND 072.209 and previous	CSTAT.072.210 – 072.224 AND 073.225 and later
CX725	CXTAT.073.022 – 073.023 AND 072.209 and previous	CXTAT.072.210 – 072.224 AND 073.225 and later
XC4140, XC4150	CXTAT.073.022 – 073.023 AND 072.209 and previous	CXTAT.072.210 – 072.224 AND 073.225 and later
CS921, CS923	CSTMH.073.022 – 073.023 AND 072.209 and previous	CSTMH.072.210 – 072.224 AND 073.225 and later
CX921, CX922, CX923, CX924	CXTMH.073.022 – 073.023 AND 072.209 and previous	CXTMH.072.210 – 072.224 AND 073.225 and later
XC92xx	CXTMH.073.022 – 073.023 AND 072.209 and previous	CXTMH.072.210 – 072.224 AND 073.225 and later
CS31x	LW75.VYL.P278 and previous	LW75.VYL.P279 and later
CS41x	LW75.VY2.P278 and previous	LW75.VY2.P279 and later
CS51x	LW75.VY4.P278 and previous	LW75.VY4.P279 and later
CX310	LW75.GM2.P278 and previous	LW75.GM2.P279 and later
CX410 & XC2130	LW75.GM4.P278 and previous	LW75.GM4.P279 and later
CX510 & XC2132	LW75.GM7.P278 and previous	LW75.GM7.P279 and later
MS310, MS312, MS317	LW75.PRL.P278 and previous	LW75.PRL.P279 and later
MS410, M1140	LW75.PRL.P278 and previous	LW75.PRL.P279 and later
MS315, MS415, MS417	LW75.TL2.P278 and previous	LW75.TL2.P279 and later
MS51x, MS610dn, MS617	LW75.PR2.P278 and previous	LW75.PR2.P279 and later
M1145, M3150dn	LW75.PR2.P278 and previous	LW75.PR2.P279 and later
MS610de, M3150	LW75.PR4.P278 and previous	LW75.PR4.P279 and later

MS810, MS811, MS812, MS817, MS818	LW75.DN2.P278 and previous	LW75.DN2.P279 and later
MS810de, M5155, M5163	LW75.DN4.P278 and previous	LW75.DN4.P279 and later
MS812de, M5170	LW75.DN7.P278 and previous	LW75.DN7.P279 and later
MS91x	LW75.SA.P278 and previous	LW75.SA.P279 and later
MX31x, XM1135	LW75.SB2.P278 and previous	LW75.SB2.P279 and later
MX410, MX510 & MX511	LW75.SB4.P278 and previous	LW75.SB4.P279 and later
XM1140, XM1145	LW75.SB4.P278 and previous	LW75.SB4.P279 and later
MX610 & MX611	LW75.SB7.P278 and previous	LW75.SB7.P279 and later
XM3150	LW75.SB7.P278 and previous	LW75.SB7.P279 and later
MX71x, MX81x	LW75.TU.P278 and previous	LW75.TU.P279 and later
XM51xx & XM71xx	LW75.TU.P278 and previous	LW75.TU.P279 and later
MX91x & XM91x	LW75.MG.P278 and previous	LW75.MG.P279 and later
MX6500e	LW75.JD.P278 and previous	LW75.JD.P279 and later
C746	LHS60.CM2.P738 and previous	LHS60.CM2.P739 and later
C748, CS748	LHS60.CM4.P738 and previous	LHS60.CM4.P739 and later
C792, CS796	LHS60.HC.P738 and previous	LHS60.HC.P739 and later
C925	LHS60.HV.P738 and previous	LHS60.HV.P739 and later
C950	LHS60.TP.P738 and previous	LHS60.TP.P739 and later
X548 & XS548	LHS60.VK.P738 and previous	LHS60.VK.P739 and later
X74x & XS748	LHS60.NY.P738 and previous	LHS60.NY.P739 and later
X792 & XS79x	LHS60.MR.P738 and previous	LHS60.MR.P739 and later
X925 & XS925	LHS60.HK.P738 and previous	LHS60.HK.P739 and later
X95x & XS95x	LHS60.TQ.P738 and previous	LHS60.TQ.P739 and later
6500e	LHS60.JR.P738 and previous	LHS60.JR.P739 and later
C734	LR.SK.P825 and previous	LR.SK.P826 and later
C736	LR.SKE.P825 and previous	LR.SKE.P826 and later
E46x	LR.LBH.P825 and previous	LR.LBH.P826 and later
T65x	LR.JP.P825 and previous	LR.JP.P826 and later
X46x	LR.BS.P825 and previous	LR.BS.P826 and later
X65x	LR.MN.P825 and previous	LR.MN.P826 and later
X73x	LR.FL.P825 and previous	LR.FL.P826 and later
W850	LP.JB.P824 and previous	LP.JB.P825 and later
X86x	LP.SP.P824 and previous	LP.SP.P825 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 Reutter of SySS GmbH 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

Revision	Date	Reason
1.1	26 June 2020	Initial Public Release