Lexmark Security Advisory:

Revision: 1.0
Last update: 20-Feb-2020
Public Release Date: 28-Feb-2020

Summary

Two Cross Site Scripting vulnerabilities have been identified in older Lexmark devices .

References

CVE: CVE-2019-19772, CVE-2019-19773

Details

CVE-2019-19772
A reflected cross site scripting vulnerability has been identified in the embedded web server used in older generation 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	

CVE-2019-19773
A stored cross site scripting vulnerability has been identified in the embedded web server used in older generation 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, including session hijacking and credential theft.

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	LW74.VYL.P267 and previous	LW74.VYL.P268 and later
CS41x	LW74.VY2.P267 and previous	LW74.VY2.P268 and later
CS51x	LW74.VY4.P267 and previous	LW74.VY4.P268 and later
CX310	LW74.GM2.P267 and previous	LW74.GM2.P268 and later
CX410 & XC2130	LW74.GM4.P267 and previous	LW74.GM4.P268 and later
CX510 & XC2132	LW74.GM7.P267 and previous	LW74.GM7.P268 and later
MS310, MS312, MS317	LW74.PRL.P267 and previous	LW74.PRL.P268 and later
MS410, M1140	LW74.PRL.P267 and previous	LW74.PRL.P268 and later
MS315, MS415, MS417	LW74.TL2.P267 and previous	LW74.TL2.P268 and later
MS51x, MS610dn, MS617	LW74.PR2.P267 and previous	LW74.PR2.P268 and later
M1145, M3150dn	LW74.PR2.P267 and previous	LW74.PR2.P268 and later
MS610de, M3150	LW74.PR4.P267 and previous	LW74.PR4.P268 and later
MS71x, M5163dn	LW74.DN2.P267 and previous	LW74.DN2.P268 and later
MS810, MS811, MS812, MS817, MS818	LW74.DN2.P267 and previous	LW74.DN2.P268 and later
MS810de, M5155, M5163	LW74.DN4.P267 and previous	LW74.DN4.P268 and later
MS812de, M5170	LW74.DN7.P267 and previous	LW74.DN7.P268 and later
MS91x	LW74.SA.P267 and previous	LW74.SA.P268 and later
MX31x, XM1135	LW74.SB2.P267 and previous	LW74.SB2.P268 and later
MX410, MX510 & MX511	LW74.SB4.P267 and previous	LW74.SB4.P268 and later
XM1140, XM1145	LW74.SB4.P267 and previous	LW74.SB4.P268 and later
MX610 & MX611	LW74.SB7.P267 and previous	LW74.SB7.P268 and later
XM3150	LW74.SB7.P267 and previous	LW74.SB7.P268 and later
MX71x, MX81x	LW74.TU.P267 and previous	LW74.TU.P268 and later
XM51xx & XM71xx	LW74.TU.P267 and previous	LW74.TU.P268 and later
MX91x & XM91x	LW74.MG.P267 and previous	LW74.MG.P268 and later
MX6500e	LW74.JD.P267 and previous	LW74.JD.P268 and later
C746	LHS60.CM2.P735 and previous	LHS60.CM2.P736 and later
C748, CS748	LHS60.CM4.P735 and previous	LHS60.CM4.P736 and later
C792, CS796	LHS60.HC.P735 and previous	LHS60.HC.P736 and later
C925	LHS60.HV.P735 and previous	LHS60.HV.P736 and later
C950	LHS60.TP.P735 and previous	LHS60.TP.P736 and later
X548 & XS548	LHS60.VK.P735 and previous	LHS60.VK.P736 and later
X74x & XS748	LHS60.NY.P735 and previous	LHS60.NY.P736 and later
X792 & XS79x	LHS60.MR.P735 and previous	LHS60.MR.P736 and later
X925 & XS925	LHS60.HK.P735 and previous	LHS60.HK.P736 and later
X95x & XS95x	LHS60.TQ.P735 and previous	LHS60.TQ.P736 and later
6500e	LHS60.JR.P735 and previous	LHS60.JR.P736 and later
C734	LR.SK.P822 and previous	LR.SK.P823 and later
C736	LR.SKE.P822 and previous	LR.SKE.P823 and later
E46x	LR.LBH.P822 and previous	LR.LBH.P823 and later
T65x	LR.JP.P822 and previous	LR.JP.P823 and later
X46x	LR.BS.P822 and previous	LR.BS.P823 and later
X65x	LR.MN.P822 and previous	LR.MN.P823 and later
X73x	LR.FL.P822 and previous	LR.FL.P823 and later
W850	LP.JB.P821 and previous	LP.JB.P822 and later
X86x	LP.SP.P821 and previous	LP.SP.P822 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

The XSS vulnerabilities may be mitigated by disabling the Embedded Web Server (EWS) in the affected devices.

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 Vidya Bhaskar Tripathi for bringing this to our attention.

Status of this Notice:

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	20-Feb-2020	Initial Public Release