Lexmark Security Advisory:

Revision: 1.0
Last update: 11 June 2020
Public Release Date: 19 June 2020

Summary

Lexmark devices' embedded web server contains a cross site request forgery attack vulnerability that allows the devices configuration to be altered without authorization.

References

CVE: CVE-2020-10095

Details

A vulnerability has been identified in the embedded web server used in Lexmark devices. The vulnerability allows the attacker to modify the configuration of the device.

CVSSv3 Base Score 6.8 (AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N)
Impact Subscore: 5.2
Exploitability Subscore: 1.6

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 the modification of the configuration of 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**
B2236	MSLSG.072.202 and previous	MSLSG.072.203 and later
MS331, MS431	MSLBD.072.202 and previous	MSLBD.072.203 and later
M1241	MSLBD.072.202 and previous	MSLBD.072.203 and later
B3442, B3340	MSLBD.072.202 and previous	MSLBD.072.203 and later
MB2236	MXLSG.072.202 and previous	MXLSG.072.203 and later
MX431, MX331	MXLBD.072.202 and previous	MXLBD.072.203 and later
MB3442	MXLBD.072.202 and previous	MXLBD.072.203 and later
MS521	MSNGM.072.202 and previous	MSNGM.072.203 and later
MS621, MS622	MSTGM.072.202 and previous	MSTGM.072.203 and later
M1246, M3250	MSTGM.072.202 and previous	MSTGM.072.203 and later

B2546, B2650	MSTGM.072.202 and previous	MSTGM.072.203 and later
MX421, MX521, MX522, MX622	MXTGM.072.202 and previous	MXTGM.072.203 and later
XM1242, XM1246, XM3250	MXTGM.072.202 and previous	MXTGM.072.203 and later
MB2546, MB2650	MXTGM.072.202 and previous	MXTGM.072.203 and later
MX321	MXNGM.072.202 and previous	MXNGM.072.203 and later
MB2338	MXNGM.072.202 and previous	MXNGM.072.203 and later
MS725, MS821	MSNGW.072.202 and previous	MSNGW.072.203 and later
MS822, MS823, MS825, MS826	MSTGW.072.202 and previous	MSTGW.072.203 and later
M5255, M5270	MSTGW.072.202 and previous	MSTGW.072.203 and later
B2865	MSTGW.072.202 and previous	MSTGW.072.203 and later
MX721, MX722, MX822, MX826	MXTGW.072.202 and previous	MXTGW.072.203 and later
XM5365, XM7355, XM7370	MXTGW.072.202 and previous	MXTGW.072.203 and later
C3426	CSLBN.072.202 and previous	CSLBN.072.203 and later
CS431	CSLBN.072.202 and previous	CSLBN.072.203 and later
CS331	CSLBL.072.202 and previous	CSLBL.072.203 and later
C3224	CSLBL.072.202 and previous	CSLBL.072.203 and later
C3326	CSLBL.072.202 and previous	CSLBL.072.203 and later
MC3426	CXLBN.072.202 and previous	CXLBN.072.203 and later
CX431	CXLBN.072.202 and previous	CXLBN.072.203 and later
MC3326, MC3224	CXLBL.072.202 and previous	CXLBL.072.203 and later
CX331	CXLBL.072.202 and previous	CXLBL.072.203 and later
CS622	CSTZJ.072.202 and previous	CSTZJ.072.203 and later
C2240	CSTZJ.072.202 and previous	CSTZJ.072.203 and later
CS421, CS521	CSNZJ.072.202 and previous	CSNZJ.072.203 and later
C2535, C2325, C2425	CSNZJ.072.202 and previous	CSNZJ.072.203 and later
CX522, CX622, CX625	CXTZJ.072.202 and previous	CXTZJ.072.203 and later
XC2235, XC4240	CXTZJ.072.202 and previous	CXTZJ.072.203 and later
MC2535, MC2640	CXTZJ.072.202 and previous	CXTZJ.072.203 and later
CX421	CXNZJ.072.202 and previous	CXNZJ.072.203 and later
MC2325, MC2425	CXNZJ.072.202 and previous	CXNZJ.072.203 and later
CX820, CX825, CX860	CXTPP.072.202 and previous	CXTPP.072.203 and later
XC6152, XC8155, XC8160	CXTPP.072.202 and previous	CXTPP.072.203 and later
CS820	CSTPP.072.202 and previous	CSTPP.072.203 and later
C6160	CSTPP.072.202 and previous	CSTPP.072.203 and later
CS720, CS725	CSTAT.072.202 and previous	CSTAT.072.203 and later
C4150	CSTAT.072.202 and previous	CSTAT.072.203 and later
CX725	CXTAT.072.202 and previous	CXTAT.072.203 and later
XC4140, XC4150	CXTAT.072.202 and previous	CXTAT.072.203 and later
CS921, CS923	CSTMH.072.202 and previous	CSTMH.072.203 and later
CX921, CX922, CX923, CX924	CXTMH.072.202 and previous	CXTMH.072.203 and later
XC92xx	CXTMH.072.202 and previous	CXTMH.072.203 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.

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	19-June-2020	Initial Public Release