Lexmark Security Advisory:

Revision: 1.1
Last update: 22 August 2022
Public Release Date: 30 August 2022

Summary

jQuery contains vulnerability that can lead to a denial of service, remote code execution, or property injection

References

CVE: CVE-2019-11358

Details

jQuery before 3.4.0 mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

CVSSv3 Base Score	6.1	(AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
Impact Subscore:	2.7	
Exploitability Subscore:	2.8	

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 remote code execution or denial of service on the affected 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
CX730, CX735	CXTMM.080.999 and previous	CXTMM.081.001 and later
XC4342, XC4352	CXTMM.080.999 and previous	CXTMM.081.001 and later
C4342, C4352	CXTMM.080.999 and previous	CXTMM.081.001 and later
CS730, CS735	CXTMM.080.999 and previous	CXTMM.081.001 and later
B2236	MSLSG.076.304 and previous	MSLSG.076.305 and later
MB2236	MXLSG.076.304 and previous	MXLSG.076.305 and later
MS331, MS431	MSLBD.076.304 and previous	MSLBD.076.305 and later
M1342	MSLBD.076.304 and previous	MSLBD.076.305 and later
B3442, B3340	MSLBD.076.304 and previous	MSLBD.076.305 and later
XM1342	MSLBD.076.304 and previous	MSLBD.076.305 and later
MX331, MX431	MXLBD.076.304 and previous	MXLBD.076.305 and later
MB3442	MXLBD.076.304 and previous	MXLBD.076.305 and later

MS321, MS421, MS521, MS621	MSNGM.076.304 and previous	MSNGM.076.305 and later
M1242, M1246	MSNGM.076.304 and previous	MSNGM.076.305 and later
B2338, B2442, B2546, B2650	MSNGM.076.304 and previous	MSNGM.076.305 and later
MS622	MSTGM.076.304 and previous	MSTGM.076.305 and later
M3250	MSTGM.076.304 and previous	MSTGM.076.305 and later
MX321	MXNGM.076.304 and previous	MXNGM.076.305 and later
MB2338	MXNGM.076.304 and previous	MXNGM.076.305 and later
MX421, MX521, MX522, MX622	MXTGM.076.304 and previous	MXTGM.076.305 and later
XM1242, XM1246, XM3250	MXTGM.076.304 and previous	MXTGM.076.305 and later
MB2442. MB2546, MB2650	MXTGM.076.304 and previous	MXTGM.076.305 and later
MS725, MS821, MS823, MS825	MSNGW.076.304 and previous	MSNGW.076.305 and later
B2865	MSNGW.076.304 and previous	MSNGW.076.305 and later
MS822, MS826	MSTGW.076.304 and previous	MSTGW.076.305 and later
M5255, M5270	MSTGW.076.304 and previous	MSTGW.076.305 and later
MX721, MX722, MX822, MX826	MXTGW.076.304 and previous	MXTGW.076.305 and later
XM5365, XM7355, XM7370	MXTGW.076.304 and previous	MXTGW.076.305 and later
MB2770	MXTGW.076.304 and previous	MXTGW.076.305 and later
C3426	CSLBN.076.304 and previous	CSLBN.076.305 and later
CS431, CS439	CSLBN.076.304 and previous	CSLBN.076.305 and later
CS331	CSLBL.076.304 and previous	CSLBL.076.305 and later
C3224, C3326	CSLBL.076.304 and previous	CSLBL.076.305 and later
C2326	CSLBN.076.304 and previous	CSLBN.076.305 and later
MC3426	CXLBN.076.304 and previous	CXLBN.076.305 and later
CX431	CXLBN.076.304 and previous	CXLBN.076.305 and later
XC2326	CXLBN.076.304 and previous	CXLBN.076.305 and later
MC3426	CXLBN.076.304 and previous	CXLBN.076.305 and later
MC3224, MC3326	CXLBL.076.304 and previous	CXLBL.076.305 and later
CX331	CXLBL.076.304 and previous	CXLBL.076.305 and later
CS622	CSTZJ.076.304 and previous	CSTZJ.076.305 and later
C2240	CSTZJ.076.304 and previous	CSTZJ.076.305 and later
CS421, CS521	CSNZJ.076.304 and previous	CSNZJ.076.305 and later
C2325, C2425, C2535	CSNZJ.076.304 and previous	CSNZJ.076.305 and later
CX522, CX622, CX625	CXTZJ.076.304 and previous	CXTZJ.076.305 and later
XC2235, XC4240	CXTZJ.076.304 and previous	CXTZJ.076.305 and later
MC2535, MC2640	CXTZJ.076.304 and previous	CXTZJ.076.305 and later
CX421	CXNZJ.076.304 and previous	CXNZJ.076.305 and later
MC2325, MC2425	CXNZJ.076.304 and previous	CXNZJ.076.305 and later
CX820, CX825, CS827, CX860	CXTPP.076.304 and previous	CXTPP.076.305 and later
XC6152, XC6153, XC8155, XC8160, XC8163	CXTPP.076.304 and previous	CXTPP.076.305 and later
CS820, CS827	CSTPP.076.304 and previous	CSTPP.076.305 and later
C6160	CSTPP.076.304 and previous	CSTPP.076.305 and later
CS720, CS725, CS727, CS728	CSTAT.076.304 and previous	CSTAT.076.305 and later
C4150	CSTAT.076.304 and previous	CSTAT.076.305 and later
CX725, CX727	CXTAT.076.304 and previous	CXTAT.076.305 and later
XC4140, XC4143, XC4150, XC4153	CXTAT.076.304 and previous	CXTAT.076.305 and later
CS921, CS923, CS927	CSTMH.076.304 and previous	CSTMH.076.305 and later
C9235	CSTMH.076.304 and previous	CSTMH.076.305 and later
CX920, CX921, CX922, CX923,	CXTMH.076.304 and previous	CXTMH.076.305 and later

CX924		
XC9225, XC9235, XC9245, XC9255, XC9265	CXTMH.076.304 and previous	CXTMH.076.305 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	21 June 2022	Initial Public Release
1.1	22 August 2022	Updated affected product list