Lexmark Security Advisory:

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

Summary

This vulnerability allows an attacker who has already compromised an affected Lexmark device to maintain persistence across reboots.

References

CVE: CVE-2022-29850

CWE: CWE-15, CWE-20

Details

Lexmark firmware is stored in a compressed read-only filesystem that is continuously integrity checked as programs are loaded into RAM for execution. This means that if a device is somehow compromised, a reboot should clear the issue from the device.

This vulnerability allows an attacker that has already compromised the device, and therefore has the ability to modify internal configuration files, to make their compromise persistent, meaning after a device is rebooted, it will remain compromised.

NOTE: This vulnerability cannot be used to compromise a device, it can only be used on a device that has already been compromised by another means.

CVSSv3 Base Score	9.8	(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)
Impact Subscore:	5.9	
Exploitability Subscore:	3.9	

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 persistent backdoor installed 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
B2236	MSLSG.081.013and previous	MSLSG.081.014 and later
MB2236	MXLSG.081.013and previous	MXLSG.081.014 and later
MS331, MS431	MSLBD.081.013and previous	MSLBD.081.014 and later
M1342	MSLBD.081.013and previous	MSLBD.081.014 and later

B3442, B3340	MSLBD.081.013and previous	MSLBD.081.014 and later
XM1342	MSLBD.081.013and previous	MSLBD.081.014 and later
MX331, MX431	MXLBD.081.013and previous	MXLBD.081.014 and later
MB3442	MXLBD.081.013and previous	MXLBD.081.014 and later
MS321, MS421, MS521, MS621	MSNGM.081.013and previous	MSNGM.081.014 and later
M1242, M1246	MSNGM.081.013and previous	MSNGM.081.014 and later
B2338, B2442, B2546, B2650	MSNGM.081.013and previous	MSNGM.081.014 and later
MS622	MSTGM.081.013and previous	MSTGM.081.014 and later
M3250	MSTGM.081.013and previous	MSTGM.081.014 and later
MX321	MXNGM.081.013and previous	MXNGM.081.014 and later
MB2338	MXNGM.081.013and previous	MXNGM.081.014 and later
MX421, MX521, MX522, MX622	MXTGM.081.013and previous	MXTGM.081.014 and later
XM1242, XM1246, XM3250	MXTGM.081.013and previous	MXTGM.081.014 and later
MB2442. MB2546, MB2650	MXTGM.081.013and previous	MXTGM.081.014 and later
MS725, MS821, MS823, MS825	MSNGW.081.013and previous	MSNGW.081.014 and later
B2865	MSNGW.081.013and previous	MSNGW.081.014 and later
MS822, MS826	MSTGW.081.013and previous	MSTGW.081.014 and later
M5255, M5270	MSTGW.081.013and previous	MSTGW.081.014 and later
MX721, MX722, MX822, MX826	MXTGW.081.013and previous	MXTGW.081.014 and later
XM5365, XM7355, XM7370	MXTGW.081.013and previous	MXTGW.081.014 and later
MB2770	MXTGW.081.013and previous	MXTGW.081.014 and later
C3426	CSLBN.081.013and previous	CSLBN.081.014 and later
CS431, CS439	CSLBN.081.013and previous	CSLBN.081.014 and later
CS331	CSLBL.081.013and previous	CSLBL.081.014 and later
C3224, C3326	CSLBL.081.013and previous	CSLBL.081.014 and later
C2326	CSLBN.081.013and previous	CSLBN.081.014 and later
MC3426	CXLBN.081.013and previous	CXLBN.081.014 and later
CX431	CXLBN.081.013and previous	CXLBN.081.014 and later
XC2326	CXLBN.081.013and previous	CXLBN.081.014 and later
MC3426	CXLBN.081.013and previous	CXLBN.081.014 and later
MC3224, MC3326	CXLBL.081.013and previous	CXLBL.081.014 and later
CX331	CXLBL.081.013and previous	CXLBL.081.014 and later
CS622	CSTZJ.081.013and previous	CSTZJ.081.014 and later
C2240	CSTZJ.081.013and previous	CSTZJ.081.014 and later
CS421, CS521	CSNZJ.081.013and previous	CSNZJ.081.014 and later
C2325, C2425, C2535	CSNZJ.081.013and previous	CSNZJ.081.014 and later
CX522, CX622, CX625	CXTZJ.081.013and previous	CXTZJ.081.014 and later
XC2235, XC4240	CXTZJ.081.013and previous	CXTZJ.081.014 and later
MC2535, MC2640	CXTZJ.081.013and previous	CXTZJ.081.014 and later
CX421	CXNZJ.081.013and previous	CXNZJ.081.014 and later
MC2325, MC2425	CXNZJ.081.013and previous	CXNZJ.081.014 and later
CX820, CX825, CS827, CX860	CXTPP.081.013and previous	CXTPP.081.014 and later
XC6152, XC6153, XC8155, XC8160, XC8163	CXTPP.081.013and previous	CXTPP.081.014 and later
CS820, CS827	CSTPP.081.013and previous	CSTPP.081.014 and later
C6160	CSTPP.081.013and previous	CSTPP.081.014 and later
CS720, CS725, CS727, CS728	CSTAT.081.013and previous	CSTAT.081.014 and later
C4150	CSTAT.081.013and previous	CSTAT.081.014 and later
CX725, CX727	CXTAT.081.013and previous	CXTAT.081.014 and later
XC4140, XC4143, XC4150,	CXTAT.081.013and previous	CXTAT.081.014 and later

XC4153		
CS921, CS923, CS927	CSTMH.081.013and previous	CSTMH.081.014 and later
C9235	CSTMH.081.013and previous	CSTMH.081.014 and later
CX920, CX921, CX922, CX923, CX924	CXTMH.081.013and previous	CXTMH.081.014 and later
XC9225, XC9235, XC9245, XC9255, XC9265	CXTMH.081.013and previous	CXTMH.081.014 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 the following people for bringing this issue to our attention:
Alex Plaskett of NCC Group EDG
Cedric Halbronn of NCC Group EDG
Aaron Adams of NCC Group EDG

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
1.1	22 June 2022	Initial Public Release