Lexmark Security Advisory:

Revision: 1.0
Last update: 10-May-2019
Public Release Date: 20-May-2019

Summary

Most older Lexmark devices have the "finger" service enabled by default. This service allows unauthenticated access to internal diagnostic information of the device. Lexmark recommends that the finger service be disabled by blocking access to TCP port 79 via the "TCP Port Access" configuration menu.

References

CVE: CVE-2019-10059

Details

The finger service (TCP port 79) is a legacy method for determining the state of a device. The finger service also allows unauthenticated access to diagnostic information from the device. Newer Lexmark products disable "Finger" by default, but on older devices the default is to enable the service. Lexmark recommends that the finger service be disabled by blocking access to TCP port 79 via the "TCP Port Access" configuration menu.

A firmware update is available which changes the default state of the finger service to "disabled" when the device is reset to factory defaults.

CVSSv3 Base Score   5.3   (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
Impact Subscore: 1.4
Exploitability Subscore: 3.9

CVSSv3 scores are calculated in accordance with CVSS version 3.0   (https://www.first.org/cvss/user-guide)

Impact

Successful exploitation of this vulnerability can lead to the disclosure of diagnostic information from 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
CS31x	LW71.VYL.P233 and previous	LW71.VYL.P234 and later
CS41x	LW71.VY2.P233 and previous	LW71.VY2.P234 and later
CS51x	LW71.VY4.P233 and previous	LW71.VY4.P234 and later
CX310	LW71.GM2.P233 and previous	LW71.GM2.P234 and later
CX410 & XC2130	LW71.GM4.P233 and previous	LW71.GM4.P234 and later

CX510 & XC2132	LW71.GM7.P233 and previous	LW71.GM7.P234 and later
MS310, MS312, MS317	LW71.PRL.P233 and previous	LW71.PRL.P234 and later
MS410, M1140	LW71.PRL.P233 and previous	LW71.PRL.P234 and later
MS315, MS415, MS417	LW71.TL2.P233 and previous	LW71.TL2.P234 and later
MS51x, MS610dn, MS617	LW71.PR2.P233 and previous	LW71.PR2.P234 and later
M1145, M3150dn	LW71.PR2.P233 and previous	LW71.PR2.P234 and later
MS610de, M3150	LW71.PR4.P233 and previous	LW71.PR4.P234 and later
MS71x, M5163dn	LW71.DN2.P233 and previous	LW71.DN2.P234 and later
MS810, MS811, MS812, MS817, MS818	LW71.DN2.P233 and previous	LW71.DN2.P234 and later
MS810de, M5155, M5163	LW71.DN4.P233 and previous	LW71.DN4.P234 and later
MS812de, M5170	LW71.DN7.P233 and previous	LW71.DN7.P234 and later
MS91x	LW71.SA.P233 and previous	LW71.SA.P234 and later
MX31x, XM1135	LW71.SB2.P233 and previous	LW71.SB2.P234 and later
MX410, MX510 & MX511	LW71.SB4.P233 and previous	LW71.SB4.P234 and later
XM1140, XM1145	LW71.SB4.P233 and previous	LW71.SB4.P234 and later
MX610 & MX611	LW71.SB7.P233 and previous	LW71.SB7.P234 and later
XM3150	LW71.SB7.P233 and previous	LW71.SB7.P234 and later
MX71x, MX81x	LW71.TU.P233 and previous	LW71.TU.P234 and later
XM51xx & XM71xx	LW71.TU.P233 and previous	LW71.TU.P234 and later
MX91x & XM91x	LW71.MG.P233 and previous	LW71.MG.P234 and later
MX6500e	LW71.JD.P233 and previous	LW71.JD.P234 and later
C746	LHS60.CM2.P705 and previous	LHS60.CM2.P706 and later
C748, CS748	LHS60.CM4.P705 and previous	LHS60.CM4.P706 and later
C792, CS796	LHS60.HC.P705 and previous	LHS60.HC.P706 and later
C925	LHS60.HV.P705 and previous	LHS60.HV.P706 and later
C950	LHS60.TP.P705 and previous	LHS60.TP.P706 and later
X548 & XS548	LHS60.VK.P705 and previous	LHS60.VK.P706 and later
X74x & XS748	LHS60.NY.P705 and previous	LHS60.NY.P706 and later
X792 & XS79x	LHS60.MR.P705 and previous	LHS60.MR.P706 and later
X925 & XS925	LHS60.HK.P705 and previous	LHS60.HK.P706 and later
X95x & XS95x	LHS60.TQ.P705 and previous	LHS60.TQ.P706 and later
6500e	LHS60.JR.P705 and previous	LHS60.JR.P706 and later
C734	LR.SK.P815 and previous	LR.SK.P816 and later
C736	LR.SKE.P815 and previous	LR.SKE.P816 and later
E46x	LR.LBH.P815 and previous	LR.JBH.P816 and later
T65x	LR.JP.P815 and previous	LR.JP.P816 and later
X46x	LR.BS.P815 and previous	LR.BS.P816 and later
X65x	LR.MN.P815 and previous	LR.MN.P816 and later
X73x	LR.FL.P815 and previous	LR.FL.P816 and later
W850	LP.JB.P815 and previous	LP.JB.P816 and later
X86x	LP.SP.P815 and previous	LP.SP.P816 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 that the finger service be disabled by blocking access to TCP port 79 via the "TCP/IP Port Access" configuration menu.

Lexmark suggests a firmware update if wish your device to disable the finger service by default when the device is reset to factory defaults.

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 Romero and Mario Rivas of NCC group 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
1.0	20-May-2019	Initial Public Release