Lexmark Security Advisory:

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

Summary

SNMP Denial of Service Vulnerability

Some Lexmark printers contain a denial of service vulnerability in their SNMP service. This vulnerability can be exploited to crash the device.

References

CVE: CVE-2019-9931

Details

A specially crafted request to the SNMP service will cause a vulnerable device to crash. If the "General Settings"->Error Recovery" setting is set to "Auto Reboot" (the default) then the device will automatically reboot until the "Max Auto Reboots" limit is reached.

CVSSv3 Base Score   7.5   (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
Impact Subscore: 3.6
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 a denial of service on the affected device by causing it to crash.

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.P230 and previous	LW71.VYL.P231 and later
CS41x	LW71.VY2.P230 and previous	LW71.VY2.P231 and later
CS51x	LW71.VY4.P230 and previous	LW71.VY4.P231 and later
CX310	LW71.GM2.P230 and previous	LW71.GM2.P231 and later
CX410 & XC2130	LW71.GM4.P230 and previous	LW71.GM4.P231 and later
CX510 & XC2132	LW71.GM7.P230 and previous	LW71.GM7.P231 and later
MS310, MS312, MS317	LW71.PRL.P230 and previous	LW71.PRL.P231 and later

MS410, M1140	LW71.PRL.P230 and previous	LW71.PRL.P231 and later
MS315, MS415, MS417	LW71.TL2.P230 and previous	LW71.TL2.P231 and later
MS51x, MS610dn, MS617	LW71.PR2.P230 and previous	LW71.PR2.P231 and later
M1145, M3150dn	LW71.PR2.P230 and previous	LW71.PR2.P231 and later
MS610de, M3150	LW71.PR4.P230 and previous	LW71.PR4.P231 and later
MS71x, M5163dn	LW71.DN2.P230 and previous	LW71.DN2.P231 and later
MS810, MS811, MS812, MS817, MS818	LW71.DN2.P230 and previous	LW71.DN2.P231 and later
MS810de, M5155, M5163	LW71.DN4.P230 and previous	LW71.DN4.P231 and later
MS812de, M5170	LW71.DN7.P230 and previous	LW71.DN7.P231 and later
MS91x	LW71.SA.P230 and previous	LW71.SA.P231 and later
MX31x, XM1135	LW71.SB2.P230 and previous	LW71.SB2.P231 and later
MX410, MX510 & MX511	LW71.SB4.P230 and previous	LW71.SB4.P231 and later
XM1140, XM1145	LW71.SB4.P230 and previous	LW71.SB4.P231 and later
MX610 & MX611	LW71.SB7.P230 and previous	LW71.SB7.P231 and later
XM3150	LW71.SB7.P230 and previous	LW71.SB7.P231 and later
MX71x, MX81x	LW71.TU.P230 and previous	LW71.TU.P231 and later
XM51xx & XM71xx	LW71.TU.P230 and previous	LW71.TU.P231 and later
MX91x & XM91x	LW71.MG.P230 and previous	LW71.MG.P231 and later
MX6500e	LW71.JD.P230 and previous	LW71.JD.P231 and later
C746	LHS60.CM2.P697 and previous	LHS60.CM2.P698 and later
C748, CS748	LHS60.CM4.P697 and previous	LHS60.CM4.P698 and later
C792, CS796	LHS60.HC.P697 and previous	LHS60.HC.P698 and later
C925	LHS60.HV.P697 and previous	LHS60.HV.P698 and later
C950	LHS60.TP.P697 and previous	LHS60.TP.P698 and later
X548 & XS548	LHS60.VK.P697 and previous	LHS60.VK.P698 and later
X74x & XS748	LHS60.NY.P697 and previous	LHS60.NY.P698 and later
X792 & XS79x	LHS60.MR.P697 and previous	LHS60.MR.P698 and later
X925 & XS925	LHS60.HK.P697 and previous	LHS60.HK.P698 and later
X95x & XS95x	LHS60.TQ.P697 and previous	LHS60.TQ.P698 and later
6500e	LHS60.JR.P697 and previous	LHS60.JR.P698 and later
C734	LR.SK.P814 and previous	LR.SK.P815 and later
C736	LR.SKE.P814 and previous	LR.SKE.P815 and later
E46x	LR.LBH.P814 and previous	LR.LBH.P815 and later
T65x	LR.JP.P814 and previous	LR.JP.P815 and later
X46x	LR.BS.P814 and previous	LR.BS.P815 and later
X65x	LR.MN.P814 and previous	LR.MN.P815 and later
X73x	LR.FL.P814 and previous	LR.FL.P815 and later
W850	LP.JB.P814 and previous	LP.JB.P815 and later
X86x	LP.SP.P814 and previous	LP.SP.P815 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

Disabling the SNMP service on the device or disabling access to TCP port 161 blocks the ability to exploit this vulnerability.

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