Lexmark Security Advisory:

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

Summary

A few older Lexmark devices did not have the ability to restrict access to the SE and shortcut menus. Therefore unauthenticated users could access this information.

References

CVE: CVE-2019-9934, CVE-2019-9935

Details

A few older Lexmark devices did not have the ability to restrict access to the SE and shortcut menus. . Therefore, unauthenticated users could access the information in these menus. The shortcut menu contains information on the shortcuts configured in the device; the SE menu contains information used by Lexmark to diagnose device errors. Neither of these menus provides access to print/scan data.

Updated firmware is available that provides the ability to restrict access to the SE and Shortcut menus.

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 information about the device configuration and operation.

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.P229 and previous	LW71.VYL.P230 and later
CS41x	LW71.VY2.P229 and previous	LW71.VY2.P230 and later
CX310	LW71.GM2.P229 and previous	LW71.GM2.P230 and later
MS310, MS312, MS317	LW71.PRL.P229 and previous	LW71.PRL.P230 and later
MS410, M1140	LW71.PRL.P229 and previous	LW71.PRL.P230 and later
MS315, MS415, MS417	LW71.TL2.P229 and previous	LW71.TL2.P230 and later
MX31x, XM1135	LW71.SB2.P229 and previous	LW71.SB2.P230 and later

MS51x, MS610dn, MS617	LW71.PR2.P229 and previous	LW71.PR2.P230 and later
M1145, M3150dn	LW71.PR2.P229 and previous	LW71.PR2.P230 and later
MS71x, M5163dn	LW71.DN2.P229 and previous	LW71.DN2.P230 and later
MS810, MS811, MS812, MS817, MS818	LW71.DN2.P229 and previous	LW71.DN2.P230 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 Daniel Romero and Mario Rivas of NCC Group for bringing this issue to our attention.

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
1.0	20-May-2019	Initial Public Release