Lexmark Security Advisory:

Revision: 1.0
Last update: January 22 2020
Public Release Date: 3 February 2021

Summary

The access control settings on a MX6500 may reset during a power on or reboot.

References

CVE: CVE-2020-35546

Details

A race condition exists while processing the state of the two security jumpers in an MX6500e. This can cause occasional misreads of the security jumper state during boot, causing the device to incorrectly believe the security jumper state has changed. The result is that security access controls may be unexpectedly reset.

CVSSv3 Base Score	4.6	(AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Impact Subscore:	3.6	
Exploitability Subscore:	0.9	

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 security access controls being reset to default values.

Affected Products

To determine a device's 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
MX6500e	LW75.JD.P296 and previous	LW75.JD.P297 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	3 February 2021	Initial Public Release