Lexmark Security Advisory:

Revision:	1.0
Last update:	20 January 2016
Public Release Date:	25 January 2016

Summary

A race condition exists detecting the security jumper state during initialization.

Under certain circumstances, during initialization, some Lexmark printers have a race condition that causes the device to incorrectly detect a change in the status of the security jumper. Depending on how the device is configured this can cause the device to remove authentication requirements to access device functions.

References

CVE:	CVE-2016-1896

Details

Lexmark has identified a race condition in some products that cause the security jumper state to be incorrectly detected during initialization. In the right conditions, the likelihood of this error occurring can be as high as 25%. If the device configuration setting: “Settings”->”Security”->”Miscellaneous”->”Security Reset Jumper” is set to “Enable Guest Access” then when the error occurs unauthenticated users will be able to access all device functions, including the ability to read/modify security settings.

The factory default configuration of the “Security Reset Jumper” setting is “Enable Guest Access”.

CVSS	Base Score	7.2		(AV:L/AC:L/AU:N/C:C/I:C/A:C)
	Impact Subscore:		10	
	Exploitability Subscore:		3.9	

CVSS scores are calculated in accordance with CVSS version 2.0   (http://www.first.org/cvss/cvss-guide.html)

Impact

Successful exploitation of this vulnerability can lead to the disclosure and/or modification of configuration information 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
CX820de, CX820dtfe	PP.02.048 and previous	PP.02.049 and later
XC6152de, XC6152dtfe	PP.02.048 and previous	PP.02.049 and later
CX825de, CX825dte, CX825dtfe	PP.02.048 and previous	PP.02.049 and later
XC8155de, XC8155dte	PP.02.048 and previous	PP.02.049 and later
CX860de, CX860dte, CX860dtfe	PP.02.048 and previous	PP.02.049 and later
XC8160de, XC8160dte	PP.02.048 and previous	PP.02.049 and later
CS820de, CS820dte, CS820dtfe	YK.02.048 and previous	YK.02.049 and later
C6160	YK.02.048 and previous	YK.02.049 and later
CS720de, CS720dte	CB.02.048 and previous	CB.02.049 and later
CS725de, CS725dte	CB.02.048 and previous	CB.02.049 and later
C4150	CB.02.048 and previous	CB.02.049 and later
CX725de, CX725dhe, CX725dthe	ATL.02.048 and previous	ATL.02.049 and later
XC4150	ATL.02.048 and previous	ATL.02.049 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 updating firmware to address this issue. Changing the configuration setting "Settings"->"Security"->"Miscellaneous"->"Security Reset Jumper" to "No Effect" can be used as a workaround, but the consequence is that access to the printer cannot be recovered in the case of failure/loss of authentication credentials.

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	25-January 2016	Initial Public Release