Lexmark Security Advisory:

Revision: 1.0
Last update: 30 March 2016
Public Release Date: 7 April 2016

Summary

Out of service maintenance memory erase may fail to erase memory.

Under certain circumstances some Lexmark printers will fail to erase stored information when requested.

References

CVE: CVE-2016-3145

Details

Lexmark recommends that when a device is being taken out of service, or being de-commissioned, that the non-volatile memory of the device be erased via the "Device"->"Maintenance"->"Erase Printer Memory" and "Device"->"Maintenance"->"Erase Hard Disk" functions. Under certain circumstances, these functions may fail, causing information to remain on the device.

A limited number of products are affected; upgrading the firmware will correct the problem.

CVSSv3 Base Score	4.2	(AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:N/A:N)
Impact Subscore:	3.6	
Exploitability Subscore:	0.6	
CVSSv2 Base Score	4.6	(AV:L/AC:L/AU:S/C:C/I:N/A:N)
Impact Subscore:	6.9	
Exploitability Subscore:	3.1	

CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss/user-guide)
CVSSv2 scores are calculated in accordance with CVSS version 2.0 (https://www.first.org/cvss/v2/guide)

Impact

This vulnerability can lead to the disclosure of configuration information and user data 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.021.062 and previous	PP.021.063 and later
XC6152de, XC6152dtfe	PP.021.062 and previous	PP.021.063 and later
CX825de, CX825dte, CX825dtfe	PP.021.062 and previous	PP.021.063 and later
XC8155de, XC8155dte	PP.021.062 and previous	PP.021.063 and later
CX860de, CX860dte, CX860dtfe	PP.021.062 and previous	PP.021.063 and later
XC8160de, XC8160dte	PP.021.062 and previous	PP.021.063 and later
CS820de, CS820dte, CS820dtfe	YK.021.062 and previous	YK.021.063 and later
C6160	YK.021.062 and previous	YK.021.063 and later
CS720de, CS720dte	CB.021.062 and previous	CB.021.063 and later
CS725de, CS725dte	CB.021.062 and previous	CB.021.063 and later
C4150	CB.021.062 and previous	CB.021.063 and later
CX725de, CX725dhe, CX725dthe	ATL.021.062 and previous	ATL.021.063 and later
XC4150	ATL.021.062 and previous	ATL.021.063 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

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	7-April 2016	Initial Public Release