Lexmark Security Advisory:

Revision: 1.0
Last update: 26 August 2016
Public Release Date: 30 August 2016

Summary

XLS parsing buffer overflow vulnerability.

A vulnerability was disclosed in the XLS parsing function that provides the potential for an attacker to execute arbitrary code on an affected system.

References

CVE: CVE-2016-4335

Details

An exploitable buffer overflow vulnerability exists in the XLS parsing function used in some Lexmark devices to print XLS documents. This vulnerability allows a remote attacker to either crash or execute arbitrary code on a vulnerable system via a print request of a crafted XLS document.

CVSSv3 Base Score 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Impact Subscore: 6.6
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 the disclosure and/or modification of information and the ability to execute code on the affected system.

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.030.072 and previous	PP.030.073 and later
XC6152de, XC6152dtfe	PP.030.072 and previous	PP.030.073 and later
CX825de, CX825dte, CX825dtfe	PP.030.072 and previous	PP.030.073 and later
XC8155de, XC8155dte	PP.030.072 and previous	PP.030.073 and later
CX860de, CX860dte, CX860dtfe	PP.030.072 and previous	PP.030.073 and later
XC8160de, XC8160dte	PP.030.072 and previous	PP.030.073 and later
CS820de, CS820dte, CS820dtfe	YK.030.072 and previous	YK.030.073 and later
C6160	YK.030.072 and previous	YK.030.073 and later

CS720de, CS720dte	CB.030.072 and previous	CB.030.073 and later
CS725de, CS725dte	CB.030.072 and previous	CB.030.073 and later
C4150	CB.030.072 and previous	CB.030.073 and later
CX725de, CX725dhe, CX725dthe	ATL.030.072 and previous	ATL.030.073 and later
XC4150, XC4140	ATL.030.072 and previous	ATL.030.073 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	25 August 2016	Initial Public Release