

Lexmark Security Advisory:

Revision: 1.0
Last update: 15 November 2011
Public Release Date: 15 November 2011

Summary

Email shortcut vulnerability

Some Lexmark Multifunction Devices allow the creation of email shortcuts that contain hidden recipients. This vulnerability can be exploited to enable unauthorized personnel to receive a covert copy of email sent by the device using the modified shortcut.

References

CVE: CVE-2011-3269

Affected Products

Selected Lexmark Laser products; for specific details see “Software Versions & Fixes”

Details

Some Lexmark products allow the creation of pre-defined email addresses (“shortcuts”) to streamline the use of functions such as “Scan to Email”. On vulnerable products it is possible to craft a shortcut that contains hidden email addresses that are not displayed to the user via the operator panel or on the embedded web server.

In the event a hidden email address is added, anyone making use of the shortcut would have their scanned data sent to additional email addresses they were unaware of, although a close examination of the header of the delivered email would reveal the additional email addresses.

Impact

Successful exploitation of this vulnerability can lead to unauthorized disclosure of data.

Vulnerability Scoring Details

CVSS Base Score 5.0

Exploitability:

Access Vector: Network
Access Complexity: Low
Authentication: None

Impact:

Confidentiality: Partial
Integrity: None
Availability: None

CVSS scores are calculated in accordance with CVSS version 2.0

Workarounds

Restrict access to the manage shortcuts functionality to trusted personnel.

The “Manage Shortcuts at the Device” and “Manage Shortcuts Remotely” function access controls can be utilized to restrict the ability to create and edit email shortcuts to authenticated and authorized personnel. For more information see your product’s User Guide or the Embedded Web Server Administrator’s Guide.

Software Versions and Fixes

Updated software that removes the vulnerability described in this advisory is available for the following devices:

Lexmark Models	Affected Releases	Fixed Releases
X950 X952 X954	LHS1.TQ.P145h and previous	LHS2.TQ.P244a and later
X940e X945e	LC.BR.P051HDs and previous	
X925de	LHS1.HK.P136l and previous	LHS2.HK.P244a and later
X860 X862 X864	LP.SP.P510b and previous	
X850 X852 X854	LC4.BE.P457S and previous	
X792de	LHS1.MR.P135l and previous	LHS2.MR.P244a and later
X782e	LC2.TO.P305cS and previous	
X772e	LC.TR.P275S and previous	
X734 X736 X738	LR.FL.P510b and previous	
X650	LR.MN.P510b and previous	
X644 X646	LC2.MC.P307aS and previous	
X642	LC2.MB.P307cS and previous	
X548de	LHS1.VK.P141i and previous	LHS2.VK.P244a and later
X546	LL.EL.P433 and previous	
X543 X544	LL.EL.P433 and previous	
X46x	LR.BS.P510b and previous	
X422	GN.AQ.P202 and previous	
X36x	LL.BZ.P433 and previous	
X34x	401.ec4 and previous	
X264	LM1.MT.P232 and previous	
W850	LP.JB.P510 and previous	
W840	LS.HA.P121S and previous	
T656	LSJ.SJ.P019S and previous	
T650 T652 T654	LR.JP.P510 and previous	
T640 T642 T644	LS.ST.P240S and previous	
T440	JX.JU.P101 and previous	
E462	LR.LBH.P510 and previous	
E460	LR.LBH.P510 and previous	
E450	LM.SZ.P113vcREF and previous	
E350	LE.PH.P121 and previous	
E340 E342	BR.H.P204 and previous	
E330 E332n E234 E234n	141.C09 and previous	
E360	LL.LBM.P429f and previous	
E260	LL.LBL.P429f and previous	
E250	LE.PM.P121 and previous	
E240n	BR.Q.P204 and previous	
E240 E238	BR.M.P204 and previous	
E232	141.009 and previous	
E230	141.609 and previous	
E120	LE.UL.P040 and previous	

C950	LHS1.TP.P145h and previous	LHS2.TP.P244a and later
C935dn	LC.JO.P051S and previous	
C925de	LHS1.HV.P129l and previous	LHS2.HV.P244a and later
C920	LS.TA.P127S and previous	
C792e	LHS1.HC.P131k and previous	LHS2.HC.P244a and later
C789 C782	LC.IO.P165aS and previous	
C770 C772	LC.CM.P027bS and previous	
C760 C762	971.001 and previous	
C734 C736	LR.SK.P510 and previous	
C546	LU.AS.P433 and previous	
C540	LL.AS.P429a and previous	
C530 C532 C534	LS.SW.P026avcS and previous	
C520 C522 C524	LS.FA.P129S and previous	
C510	891.004 and previous	
6500e	LJR.JR.P169 and previous	
25xxN	LCL.CU.P106 and previous	

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.

Exploitation and Public Announcements

Lexmark is not aware of any malicious use 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

<u>Revision</u>	<u>Date</u>	<u>Reason</u>
1.0	15-Nov-2011	Initial Publication