Lexmark Security Advisory:

Revision: 1.1
Last update: 23 July 2021
Public Release Date: 9 February 2012

Summary

Information leakage vulnerability

Some Lexmark Multifunction Devices include sensitive configuration values in exported settings files. This vulnerability can be exploited to enable unauthorized disclosure of device configuration information.

References

CVE: CVE-2011-4538

Affected Products

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

Details

Some Lexmark products allow the configuration of authentication credentials, including passwords, for use when delivering email. On vulnerable products this password information is included in exported settings files.

Anyone who can request the printer export its settings, or access previously exported settings files, can obtain the full authentication credentials the device uses to deliver email.

Impact

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

Vulnerability Scoring Details

CVSS Base Score 5.0

Exploitability:		Impact:	
Access Vector:	Network	Confidentiality:	Partial
Access Complexity:	Low	Integrity:	None
Authentication:	None	Availability:	None

CVSS scores are calculated in accordance with CVSS version 2.0

Workarounds

Restrict access to the export settings functionality to trusted personnel.

The "Settings Menu at the Device" and "Settings Menu Remotely" function access controls can be utilized to restrict the ability to export settings 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
X860, X862, X864	LP.SP.P108 and previous	LP.SP.P209 and later
X734, X736, X738	LR.FL.P224c and previous	LR.FL.P311e and later
X651, X652, X654, X656, X658	LR.MN.P224a and previous	LR.MN.P311e and later
X543, X544, X546	LL.EL.P511 and previous	
X463, X464, X466	LR.BS.P224a and previous	LR.BS.P311e and later
X363, X364	LL.BZ.P511 and previous	
W850	LP.JB.P108 and previous	LP.JB.P209 and later
T650, T652, T654	LR.JP.P224a and previous	LR.JP.P311e and later
E460, E462	LR.LBH.P224a and previous	LR.LBH.P311e and later
E360	LL.LBM.P511 and previous	
E260	LL.LBL.P511 and previous	
C734, C736	LR.SK.P224a and previous	LR.SK.P311e and later
C546	LU.AS.P511 and previous	
C540, C543, C544	LL.AS.P511 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. Information about this vulnerability has been published by others.

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	2-Feb-2012	Initial Publication
1.1	23-July-2021	Updated legal notice