Lexmark Security Advisory:

Revision: 2.1
Last update: 19 July 2021
Public Release Date: 31 Jan 2014

Summary

Password reset vulnerability

Some older Lexmark Printers and MarkNet devices will fail to authenticate a specially crafted password reset request. This vulnerability can be exploited to bypass authentication configured on the device.

References

CVE: CVE-2013-6032

Affected Products

Selected Lexmark Laser printer products and MarkNet devices; for specific details see "Software Versions & Fixes"

Details

Some older Lexmark Printers and MarkNet devices provide a simple "Password Protect" feature to authorize access to device menus. On vulnerable devices it is possible to craft an HTML request to change these passwords that will bypass authentication, allowing the passwords to be changed or removed.

Impact

Successful exploitation of this vulnerability can lead to unauthorized disclosure and/or modification of printer settings.

Vulnerability Scoring Details

CVSS Base Score 9.0
Impact Subscore: 8.5
Exploitability Subscore: 10

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

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

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
X94x	LC.BR.P141 and previous	LC.BR.P142 and later
X85x	LC4.BE.P487 and previous	Contact Lexmark
X644 & X646	LC2.MC.P373 and previous	LC2.MC.P374 and later
X642	LC2.MB.P318 and previous	Contact Lexmark
W840	LS.HA.P252 and previous	Contact Lexmark
T64x	LS.ST.P346 and previous	LS.ST.P347 and later
X64xef	LC2.TI.P325 and previous	Contact Lexmark
C935dn	LC.JO.P091 and previous	Contact Lexmark
C920	LS.TA.P152 and previous	Contact Lexmark
C78x	LC.IO.P187 and previous	Contact Lexmark
X78x	LC2.IO.P335 and previous	Contact Lexmark
C77x	LC.CM.P052 and previous	Contact Lexmark
X772	LC2.TR.P291 and previous	Contact Lexmark
C53x	LS.SW.P069 and previous	Contact Lexmark
C52x	LS.FA.P150 and previous	Contact Lexmark
25xxN	LCL.CU.P114 and previous	Contact Lexmark
N4000	LC.MD.P119 and previous	Contact Lexmark
N4050e	GO.GO.N206 and previous	Contact Lexmark
N70xxe	LC.CO.N309 and previous	Contact Lexmark
E450	LM.SZ.P124 and previous	Contact Lexmark
E350	LE.PH.P129 and previous	Contact Lexmark
E250	LE.PM.P126 and previous	Contact Lexmark

Workarounds

Disabling the HTTP service (Embedded Web Server) on the device blocks the ability to exploit this vulnerability.

If the HTTP service must be left enabled, the problem can be mitigated by restricting the network devices that are permitted to communicate with the device. This can be accomplished by utilizing either the “Restricted Server List” feature, or via IPsec configuration on devices that support these features. Restricting the number of devices that can communicate with the printer limits the devices that can attempt to exploit the vulnerability.

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

Lexmark would like to thank Jeff Popio and the CERT Coordination Center for bringing this issue to our attention.

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	31-Jan-2014	Initial Public Release
2.0	11-Mar-2014	PE-release update for T64x
2.1	19-July-2021	Updated legal notice