Lexmark Security Advisory:

Revision: 1.1
Last update: 19 July 2021
Public Release Date: 31 Jan 2014

Summary

HTML injection vulnerability in “Contact” and “Location” settings

Some older Lexmark Printers do not properly sanitize user supplied values for the “Contact” and “Location” settings. The contents of these settings will be processed by a browser as HTML.
This vulnerability can be exploited to execute arbitrary HTML or script code in the browser of anyone viewing the devices embedded web server.

References

CVE: CVE-2013-6033

Affected Products

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

Details

Lexmark products provide a setting for “Location” and “Contact” information that can be modified by the user. These settings can be modified via SNMP commands or the Embedded Web Server (EWS), and are displayed on the header of most EWS pages. Affected devices do not properly sanitize the information in these fields, therefore any HTML tags, including script tags, stored in these fields will be executed in the context of the browser viewing the EWS pages.

Impact

Successful exploitation of this vulnerability can lead to compromise of the viewer’s browser sessions.

Vulnerability Scoring Details

CVSS	Base Score	4.9
	Impact Subscore:	4.9
	Exploitability Subscore:	6.8

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

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
W840	LS.HA.P252 and previous	Contact Lexmark
T64x	LS.ST.P343 and previous	LS.ST.P344 and later
C935dn	LC.JO.P091 and previous	Contact Lexmark
C920	LS.TA.P152 and previous	Contact Lexmark
C53x	LS.SW.P069 and previous	Contact Lexmark
C52x	LS.FA.P150 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 one or more of the following:

- Restricting the network devices that are permitted to communicate with the device. This can be accomplished by utilizing IPsec configuration on devices that support this feature. Restricting the number of devices that can communicate with the printer limits the devices that can attempt to exploit the vulnerability.
- Configure SNMP to disable, or require authentication, before allowing a SNMP variable to be set.
- Configure the device to require authentication when accessing the Settings menu via the EWS or operator panel.

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:

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
1.1	19-July-2021	Updated legal notice