Lexmark Security Advisory:

Revision: 1.0
Last update: 28 January 2019
Public Release Date: 28 January 2019

Summary

Information exposure of network credentials in Scan to Network app in some Lexmark devices.

References

CVE: CVE-2017-13771

Details

Older versions of the “Scan to Network” eSF application displayed network folder authentication credentials in plaintext. Therefore these credentials are disclosed when an authorized user viewed the application’s configuration page.

CVSSv3 Base Score	6.5	(AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)
Impact Subscore:	3.6	
Exploitability Subscore:	2.8	

CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss/user-guide)

Impact

This vulnerability leads to the disclosure of the authentication credentials of the network resource.

Affected Products

All versions of the “Scan to Network” application prior to 3.7.6 are affected.

To determine if the “Scan to Network” application is installed in your device, use the embedded web server to select the “Settings”->”Apps”->”Apps Management” menu (Apps menu on newer devices). If “Scan to Network” is listed, the app is installed, to determine the version expand the “Scan to Network” sub-menu.

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 the affected application 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	28 January 2019	Initial Public Release