Lexmark Security Advisory:

Revision: 1.0
Last update: 4 March 2022
Public Release Date: 15 March 2022

Summary

The initial admin account setup wizard on Lexmark devices allows unauthenticated access to the “Firmware Updates” feature.

References

CVE: CVE-2022-24935

ZDI: ZDI-CAN-15981

Details

The initial setup menus on many Lexmark devices do not restrict access to the “Firmware Updates” feature. This allows an unauthenticated attacker to downgrade the firmware installed on the device.

Lexmark recommends that you confirm your system is properly configured by following the instructions in the ”Workarounds” section below.

CVSSv3 Base Score	7.5	(AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
Impact Subscore:	3.6	
Exploitability Subscore:	3.9	

CVSSv3 scores are calculated in accordance with CVSS version 3.1 (https://www.first.org/cvss/user-guide)

Impact

Successful exploitation of this vulnerability will result in a firmware downgrade of the device. This will expose the device to vulnerabilities in older firmware.

Workarounds

To protect devices from this issue, remove public access to the “Firmware Updates” Function Access Control.

The Function Access Control settings on older devices differ significantly from modern devices (2016 and later). If the instructions for the modern devices do not match your device, use the instructions for older devices. If you need further assistance contact Lexmark’s Technical Support Center at http://support.lexmark.com to find your local support center.

Modern Devices (2016 and later):

To prevent public access to the “Firmware Updates” feature on a device, perform the following steps:

1. Go to “Settings” > “Security” from the device’s web page (embedded web server)

2. Under the “Public” Login Method, select the “Manage Permissions” link (after doing this, the web page will refresh and display Access Controls)
3. Expand the “Device Management” list
    - Uncheck “Firmware Updates”
4. Click the “Save” button

To fully protect unauthenticated access to the “Firmware Updates” feature on a device, perform the following:

1. Go to “Settings” > “Security” from the device’s web page (embedded web server)
2. Under the “Local Accounts” and/or “Network Accounts” Login Method, select the “Manage Groups/Permissions” link (after doing this, the web page will refresh and display a list of Group names)
3. Click the name of a non-administrator group (users who should not have access to the “Firmware Updates” function)
4. Expand the “Device Management” list
    - Uncheck “Firmware Updates”
5. Click the “Save” button
6. Repeat steps 2 thru 6 for each non-administrator group.

Older Devices

To fully protect unauthenticated access to the “Firmware Updates” feature on a device, perform the following steps:

1. Go to “Settings”->“Security”->”Security Setup”
2. Select either to apply a “Basic Security Setup” or follow the steps under “Advanced Security Setup” to create a security account/template
   (NOTE: additional info on security setup can be found in the Embedded Web Server Administrator’s Guide on http://support.lexmark.com. If security accounts already exist on the device, skip this step.)
3. Under the “Advanced Security Setup” section, click “Access Controls”
4. Under the “Edit Access Controls” menu, expand the “Management” submenu, protect the "Firmware Updates” function access control with an administrative account template
5. Click the “Submit” button

Exploitation and Public Announcements

Lexmark is not aware of any malicious use against Lexmark products of the vulnerability described in this advisory.

Lexmark would like to thank the following people working with Trend Micro's Zero Day Initiative (ZDI) for bringing this issue to our attention:

Chris Anastasio
Justin Taft

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	15 March 2022	Initial Public Release