Lexmark Security Advisory:

Revision: 1.0
Last update: 12 January 2022
Public Release Date: 18 January 2022

Summary

The initial admin account setup wizard on Lexmark devices allow unauthenticated access to the "out of service erase" feature.

References

CVE: CVE-2021-44736

ZDI: ZDI-CAN-15800, ZDI-CAN-15858

Details

The initial setup menus on many Lexmark devices do not restrict access to the "out of service erase" feature. This allows an unauthenticated attacker to wipe the configuration of the device.

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

CVSSv3 Base Score   9.1   (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H)
Impact Subscore: 5.2
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 reset the device to factory defaults, wiping all configuration information, including security access controls, from the device.

Workarounds

To protect devices from this issue, remove public access to the "out of service erase" 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 "out of service erase" 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 "Administrative Menus" list
   - Uncheck "Function Configuration Menus"
4. Expand the "Device Management" list
   - Uncheck "Out of Service Erase"
5. Click the "Save" button

To fully protect unauthenticated access to the "out of service erase" 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 "out of service erase" function)
4. Expand the "Administrative Menus" list
   - Uncheck the "Function Configuration Menus"
5. Expand the "Device Management" list
   - Uncheck "Out of Service Erase"
6. Click the "Save" button
7. Repeat steps 2 thru 6 for each non-administrator group.

Older Devices
   To fully protect unauthenticated access to the "out of service erase" 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 all submenus if possible), protect the following function access controls with an administrative account template:
      - "Security Menu at the Device"
      - "Security Menu Remotely"
      - "Configuration Menu"
   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:

David Berard of SYNACKTIV
Vincent Fargues of SYNACKTIV
Thomas Imbert of SYNACKTIV
Benjamin Grap of CrowdStrike Intelligence
Hanno Heinrichs of CrowdStrike Intelligence
Lukas Kupczyk of CrowdStrike Intelligence

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	12 January 2022	Initial Public Relase