Lexmark Security Advisory:

Summary

Lexmark has identified a vulnerability in our Lexmark Print Management Client (LPMC).

References

CVE: CVE-2025-1126

CWE: CWE-807

Details

A Reliance on Untrusted Inputs in a Security Decision vulnerability has been identified in the Lexmark Print Management Client.

CVSSv3 Base Score: 9.3 (AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

Impact Subscore: 6.0

Exploitability Subscore: 2.5

Affected Products

The vulnerability exists in LPMC 3.0.0 through 3.4.0. If the LPMC version falls into this range, upgrade to version 3.5.0 or later.

Obtaining Updated Software

Customers can download the latest LPMC release through the Lexmark Cloud web portal.

Workarounds

Lexmark recommends updating the LPMC version if affected.

Exploitation and Public Announcements

Lexmark is not aware of any malicious use of the vulnerability described in this disclosure.

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

The final advisory will be 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
1.1	22 December 2024	Initial Draft
1.2	10 February 2025	Updated CVE number due to collision. Previously published as CVE-2024-11348.

The vulnerability exists in Windows, Mac, and Linux clients. The vulnerability is present in all LPMC releases from LPMC 3.0.0 – LPMC 3.4.0.

An attacker could exploit this vulnerability to achieve the following:

- Launch arbitrary processes under the SYSTEM or root context, depending on operating system
- Delete folders on the workstation, including folders that require typically Administrator or other elevated permissions to access

Lexmark has released LPMC 3.5.0 to address this issue.

Action Required:

Lexmark strongly recommends that all customer currently using LPMC 3.0 through 3.4.0 update immediately to address this issue.

We apologize for any inconvenience this may cause and appreciate your prompt attention to this matter. If you have any questions or need assistance, please contact your Lexmark account team or contact the Technical Support Center. Contact information is available at https://support.lexmark.com/en_us/contact-support.html