

Lexmark Security Advisory:

Revision: 1.0
Last update: June 29 2021
Public Release Date: July 2 2021

Summary

The Lexmark Printer Software G2, G3 and G4 Installation Packages have a local escalation of privilege vulnerability due to a registry entry that has an unquoted service path.

References

CVE: CVE-2021-35469
CWE-428

Details

The Windows version of the Lexmark Printer Software G2, G3 and G4 Installation Packages install a service named LM__bdsvc that runs with system privileges. Unpatched versions of the installation packages do not quote the fully qualified path name for the LM__bdsvc executable during installation. Since the installation path is in the directory “C:\Program Files\...” if an attacker installed a program named “C:\Program” it would execute, with SYSTEM privileges, when the system attempts to launch the LM__bdsvc service.

Updating the G2, G3 or G4 Installation Packages will correct the issue.

The LM__bdsvc service is used by the Lexmark “Status Center” application to communicate to Lexmark printers over USB. LM__bdsvc is only installed if the Lexmark “Status Center” application is installed.

CVSSv3 Base Score	7.8	(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Impact Subscore:	5.9	
Exploitability Subscore:	1.8	

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

Impact

Successful exploitation of this vulnerability can lead to attacker-controlled code running with SYSTEM privileges.

Affected Products

Lexmark Printer Software G2 Installation Package 1.8.0.0 and previous versions.
Lexmark Printer Software G3 Installation Package 1.2.0.0 and previous versions.
Lexmark Printer Software G4 Installation Package 1.3.0.0 and previous versions.

Obtaining Updated Software

To obtain Lexmark Printer Software G2, G3 or G4 Installation Package version 1.9.0.0, please visit:

- Lexmark Printer Software G2 Installation Package version 1.9.0.0
https://www.lexmark.com/content/iss/www-lexmark-com/en_us/support/download.DRI1000415.html
- Lexmark Printer Software G3 Installation Package version 1.3.0.0
https://www.lexmark.com/content/iss/www-lexmark-com/en_us/support/download.DRI1000416.html
- Lexmark Printer Software G4 Installation Package version 1.4.0.0
https://www.lexmark.com/content/iss/www-lexmark-com/en_us/support/download.DRI1000417.html

Otherwise contact Lexmark's Technical Support Center at <http://support.lexmark.com> to find your local support center.

Workarounds

Lexmark recommends updating the application if you have a vulnerable version, but the following workaround can be utilized as a temporary measure.

If updating the application is not possible, manually editing the "ImagePath" registry entry in the "Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LM__bdsvc" registry key to add quotes around the fully qualified path name will resolve the issue.

Exploitation and Public Announcements

Lexmark is not aware of any malicious use 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

<u>Revision</u>	<u>Date</u>	<u>Reason</u>
1.0	29 June 2021	Initial Public Release