Lexmark Security Statement

Revision: 1.0
Last update: 6 April 2022
Public Release Date: 6 April 2022

Summary

Spring Framework is an open-source framework for building enterprise Java applications. Because the severity of the vulnerability is critical (CVSS score: pending), CVE-2022-22965 is given the name SpringShell (and/or Spring4Shell). Spring is widely used in the industry by various programs and systems.

References

CVE: CVE-2022-22965

CVS: CVE-2022-22963

Details

Two vulnerabilities were recently announced within the Spring Framework, an open-source framework for building enterprise Java applications.

March 29, 2022: The Spring Cloud Expression Resource Access Vulnerability tracked in CVE-2022-22963 was patched with the release of Spring Cloud Function 3.1.7 and 3.2.3.

March 31, 2022: Spring released version 5.3.18 and 5.2.20 of Spring Framework to patch another more severe vulnerability tracked in CVE-2022-22965. The CVE-2022-22965 vulnerability allows an attacker unauthenticated remote code execution (RCE). The exploitation of this vulnerability could result in a webshell being installed onto the compromised server that allows further command execution.

Impact

Based on the required criteria for exploit of Spring4Shell (CVE-2022-22965), **Lexmark has determined our hardware and software products are not impacted.**

For additional details, please reference the table in the Product Impact Summary. Any product that is not listed in this table is still under review for impact. This table will be revised as new information is available.

Product Impact Summary

Product	Impacted (Yes/No)	Remedy	Status	Upgrade Path
Hardcopy Printers and MFPs	No	N/A	Does not use Spring Framework	N/A
Publishing Platform for Retail	No	N/A	Does not use JAVA apps	N/A
Lexmark Cloud Services (LCS) Fleet Agent	No	N/A	Does not use Spring Framework	N/A
Lexmark Cloud Services (LCS) Services	No	N/A	Does not use WAR files, not impacted by CVE	N/A
Lexmark Cloud Services (LCS) Clients	No	N/A	Some clients do not use JAVA apps or Spring Framework and others are not impacted by CVE.	N/A
MVE (Markvision Enterprise)	No	N/A	Uses Java 8 LTS, not impacted by CVE	N/A
LFT	No	N/A	Uses Java 8 LTS, not impacted by CVE	N/A
LRAM	No	N/A	Does not use Spring Framework	N/A
LDCM (Lexmark Data Collection Manager) v6.x	No	N/A	Does not use JAVA apps	N/A
LDCM (Lexmark Data Collection Manager) v7.x	No	N/A	Does not use JAVA apps	N/A
LRMe (Lexmark Remote Management Extension)	No	N/A	Uses JAVA 8 LTS, not impacted by CVE	N/A
LDD (Lexmark Document Distributor)	No	N/A	Uses JAVA 8 LTS, not impacted by CVE	N/A
LPM (Lexmark Print Management)	No	N/A	Uses JAVA 8 LTS, not impacted by CVE	N/A
DDU (Device Deployment Utility)	No	N/A	Uses JAVA 8 LTS, not impacted by CVE	N/A

Obtaining Updated Software

Not applicable

Workarounds

Not applicable

Exploitation and Public Announcements

Lexmark is not aware of any malicious use against Lexmark products of the vulnerabilities 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 statement is posted on Lexmark's website 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	6 April 2022	Initial Public Release