Lexmark Security Advisory:

Revision: 1.6
Last update: 25 January 2022
Public Release Date: 16 December 2021

Summary

Log4j is a commonly used piece of code that helps software applications keep track of their past activities. Instead of re-creating a logging component each time a developer builds new software, they often use existing code like log4j. It's free on the Internet and very widely used, appearing in many Internet Services. Log4j has been found to be vulnerable and details regarding the vulnerabilities are outlined below.

References

CVE: CVE-2021-44228

CVE: CVE-2021-45046

CVE: CVE-2021-45105

Details

The Apache Log4j utility is an open-source Apache framework that is a commonly used component for logging requests. On December 9, 2021, a vulnerability was reported that could allow a system running Apache Log4j version 2.14 or below to be compromised and allow an attacker to execute arbitrary code on the vulnerable server. On December 10th, 2021, NIST (National Institute of Standards and Technology) published a critical CVE (Common Vulnerabilities and Exposures) in the National Vulnerability Database identifying this as CVE-2021-44228. The official CVSS (Common Vulnerability Scoring System) base severity score has been determined as a severity of 10. The latest guidance from the Apache Software Foundation is to upgrade to 2.17. The latest CVE and guidance from the Apache Software Foundation is available here: https://nvd.nist.gov/vuln/detail/CVE-2021-45105 and https://logging.apache.org/log4j/2.x/security.html

Impact

Lexmark development teams have assessed Lexmark solutions and are now actively implementing remediation plans for the Log4j vulnerability on any Lexmark solutions impacted. We share your sense of urgency and are working diligently to incorporate the necessary solutions to address the issue.

The table below lists Lexmark products that may be impacted by the Log4j vulnerability (CVE-2021-44228, CVE-2021-45046 and CVE-2021-45105). 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 MFP's	No	N/A	No further action needed	N/A
Publishing Platform for Retail	No	N/A	No further action needed	N/A
LCS Fleet Agent v1.2.46	Yes	Yes	LCS Notifications LCS New and Changed Functionality	See instructions in the status section
LCS Printer Enrollment Tool 2.7.0-2	Yes	Yes	LCS Notifications LCS New and Changed Functionality	See instructions in the status section
MVE (Markvision Enterprise)	Yes	MVE 4.1.1 or above	Lexmark Markvision Enterpise (homepage)	Customer Installer
LFT/LRAM	Yes	Yes	Update Available	Customer Installer
LDCM (Lexmark Data Collection Manager) v6.x	No	N/A	No further action required	N/A
LDCM (Lexmark Data Collection Manager) v7.x	Yes	Yes	Workaround Available	Tech Ops Engagement
LRMe (Lexmark Remote Management Extension)	Yes	Yes	Update Available	Tech Ops Engagement
LDD (Lexmark Document Distributor)	Yes	Yes	Update and Workaround Available	NA - SD&I - Contact TPM, Other Geos – Contact Lexmark Technical Support
LPM (Lexmark Print Management)	Yes	Yes	Update and Workaround Available	NA - SD&I - Contact TPM, Other Geos – Contact Lexmark Technical Support
DDU (Device Deployment Utility)	Yes	DDU 2.12 or above	Lexmark Device Deployment Utility (support site) or DDU 2.12 Egnyte Site	Customer Installer
VSC (Virtual Solution Center)	Yes	EOL – Jan 28	Customers required to use CFM or Package Builder	Use CFM or Package Builder

Obtaining Updated Software

To obtain firmware that resolves this issue or if you have special code, please contact Lexmark's Technical Support Center at http://support.lexmark.com to find your local support center.

Workarounds

Lexmark recommends an update to the impacted components.

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 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	16 December 2021	Initial Public Release
1.1	20 December 2021	Added CVE-2021-45046
1.2	21 December 2021	Added CVE-2021-45105 and provided a significant update on investigation into several software products
1.3	23 December 2021	Several updates on status and added additional impacted software products
1.4	5 January 2022	Updated LDCM to clarify v6.x was not impacted and created new entry for LDCM 7.x
1.5	18 January 2022	Updated status for LDD and LPM
1.6	25 January 2022	Updated document format