Lexmark Security Advisory:

Revision:	1.2
Last update:	19 July 2021
Public Release Date:	15 April 2014

Summary

OpenSSL Heartbeat Vulnerability

Lexmark has learned of a vulnerability in certain versions of the open-source OpenSSL Library that allows unauthenticated access to private memory of printer devices and computer systems.

Multiple Lexmark products are affected by this vulnerability.

This advisory will be updated as additional information becomes available

References

CVE: CVE-2014-0160

Details

On April 8, 2014 a vulnerability, commonly referred to as "Heartbleed" was announced in the open-source software package OpenSSL. Some versions of OpenSSL contain a flaw in its implementation of the TLS/DTLS heartbeat functionality. This flaw allows an attacker to access private memory of the application that uses the vulnerable OpenSSL library. This access may lead to the disclosure and compromise of authentication credentials (usernames/passwords, private keys, etc.) as well as user data.

Vulnerability Scoring Details

CVSS Base Score	5.0	
Impact Subscore:		2.9
Exploitability Subscore:		10

Exploitability:		Impact:	
Access Vector:	Network	Confidentiality:	Partial
Access Complexity:	Low	Integrity:	None
Authentication:	None	Availability:	None

CVSS scores are calculated in accordance with CVSS version 2.0 (http://www.first.org/cvss/cvss-guide.html)

Impact

The impact of this vulnerability varies depending on the affected product.

Unaffected Products

The following products have been investigated and are not affected by this vulnerability:

- Virtual Solutions Center
- Cloud Deployment Platform
- SmartSolutions
- MarkVision Enterprise
- Managed Print Services / Lexmark Data Collection Manager

We have confirmed that Perceptive Software products are not affected by this vulnerability.

Affected Products

The following products are known to be affected, for specific details see “Product Specific Information” below. Lexmark is assessing each product and will update this advisory as more information becomes available.

- Selected Laser printer products
- Lexmark Document Distributor
- Lexmark Print Management, On-Premise
- Lexmark Fleet Manager
- Cloud Configuration Services

Product Specific Information

Lexmark is individually assessing each product and will update this advisory as more information becomes available.

Laser printer products

The following printers and MFPs are affected:

To determine what level of firmware a devices is running, select the “Reports”->”Menu Setting Page” menu item from the operator panel. If the firmware is listed under “Affected Releases”, upgrade to a “Fixed Release”.

Lexmark Models	**Affected Releases**	**Fixed Releases**
CS310	LW20.VYL.P231 thru LW30.VYL.P355	LW30.VYL.P356 and later
CS410	LW20.VY2.P231 thru LW30.VY2.P355	LW30.VY2.P356 and later
CS510	LW20.VY4.P231 thru LW30.VY4.P355	LW30.VY4.P356 and later
CX310	LW20.GM2.P231 thru LW30.GM2.P355	LW30.GM2.P356 and later
CX410	LW20.GM4.P231 thru LW30.GM4.P355	LW30.GM4.P356 and later
CX510	LW20.GM7.P231 thru LW30.GM7.P355	LW30.GM7.P356 and later
XC2132	LW20.GM7.P231 thru LW30.GM7.P355	LW30.GM7.P356 and later
MS310	LW20.PRL.P231 thru LW30.PRL.P355	LW30.PRL.P356 and later
MS410	LW20.PRL.P231 thru LW30.PRL.P355	LW30.PRL.P356 and later
MS510	LW20.PR2.P231 thru LW30.PR2.P355	LW30.PR2.P356 and later
MS610dn & MS610dtn	LW20.PR2.P231 thru LW30.PR2.P355	LW30.PR2.P356 and later

M1145 & M3150dn	LW20.PR2.P231 thru LW30.PR2.P355	LW30.PR2.P356 and later
MS610de & MS610dte	LW20.PR4.P231 thru LW30.PR4.P355	LW30.PR4.P356 and later
M3150	LW20.PR4.P231 thru LW30.PR4.P355	LW30.PR4.P356 and later
MS71x	LW20.DN2.P231 thru LW30.DN2.P355	LW30.DN2.P356 and later
MS810n, MS810dn & MS810dtn	LW20.DN2.P231 thru LW30.DN2.P355	LW30.DN2.P356 and later
MS811	LW20.DN2.P231 thru LW30.DN2.P355	LW30.DN2.P356 and later
MS812dn, MS812dtn	LW20.DN2.P231 thru LW30.DN2.P355	LW30.DN2.P356 and later
M5163dn	LW20.DN2.P231 thru LW30.DN2.P355	LW30.DN2.P356 and later
MS810de	LW20.DN4.P231 thru LW30.DN4.P355	LW30.DN4.P356 and later
M5155 & M5163	LW20.DN4.P231 thru LW30.DN4.P355	LW30.DN4.P356 and later
MS812de	LW20.DN7.P231 thru LW30.DN7.P355	LW30.DN7.P356 and later
M5170	LW20.DN7.P231 thru LW30.DN7.P355	LW30.DN7.P356 and later
MX310	LW20.SB2.P231 thru LW30.SB2.P355	LW30.SB2.P356 and later
MX410, MX510 & MX511	LW20.SB4.P231 thru LW30.SB4.P355	LW30.SB4.P356 and later
XM1145	LW20.SB4.P231 thru LW30.SB4.P355	LW30.SB4.P356 and later
MX610 & MX611	LW20.SB7.P231 thru LW30.SB7.P355	LW30.SB7.P356 and later
XM3150	LW20.SB7.P231 thru LW30.SB7.P355	LW30.SB7.P356 and later
MX71x	LW20.TU.P231 thru LW30.TU.P355	LW30.TU.P356 and later
MX81x	LW20.TU.P231 thru LW30.TU.P355	LW30.TU.P356 and later
XM51xx & XM71xx	LW20.TU.P231 thru LW30.TU.P355	LW30.TU.P356 and later
MX6500e	LF20.JD.P231 thru LF30.JD.P355	LF30.JD.P356 and later

Note: Releases prior to P231 were not affected.

Only the devices listed above are affected, all other devices are not affected.

The benefit of generating new device keys and certificates is dependent on the environment in which the device is deployed. If device certificates (self-signed and/or PKI signed) are utilized within the environment, it is suggested that customers evaluate the need to generate new keys and certificates based on their internal risk assessment.

Workarounds

Lexmark recommends a firmware update if your device has affected firmware.

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.

Lexmark Document Distributor

Applications running on Lexmark Document Distributor (LDD) versions 4.7 & 4.8 are vulnerable, all earlier versions of LDD not affected by this vulnerability. A patch is available for the vulnerable versions of LDD that upgrades the OpenSSL library to version 1.0.1g.

Workarounds

Lexmark recommends applying the patch if you have a vulnerable version.

Obtaining Updated Software

To obtain the patch and installation instructions to resolve this issue, please contact your Lexmark Solutions Help Desk.

Lexmark Print Management, On-Premise

The on-premise version of the Lexmark Print Management application runs on LDD, therefore it is vulnerable when running on LDD versions 4.7 or 4.8. A patch is available for LDD that fixes the vulnerability, for details, see the section on Lexmark Document Distributor above.

Workarounds

Lexmark recommends applying the patch if you have a vulnerable version.

Obtaining Updated Software

To obtain software and installation instructions to resolve this issue, please contact your Lexmark Solutions Help Desk.

Lexmark Fleet Manager

Lexmark Fleet Manager 3.0 is not vulnerable, but Lexmark Fleet Manager 2.0 is.

An updated version of LFM 2.0 that fixes the vulnerability has been posted, and is available for immediate or automatic updating. The fixed versions of the affected LFM components are:

Lexmark Service Monitor:	2.27.4.0.29
Lexmark Fleet Tracker:	2.27.4.0.28

Workarounds

Lexmark recommends updating the affected components if you have a vulnerable version.

Obtaining Updated Software

Updates for Lexmark Fleet Manager 2.0 are automatically distributed via the activation server. To obtain instructions on how to perform manual update, please contact Lexmark’s Technical Support Center at http://support.lexmark.com to find your local support center.

Exploitation and Public Announcements

Lexmark is aware of unconfirmed reports of 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

Revision	Date	Reason
1.0	15 -April-2014	Initial Public Release
1.1	18 -April-2014	Updated information on software and services
1.2	19-July-2021	Updated legal notice