Lexmark Security Advisory:

Revision:	1.2
Last update:	19 July 2021
Public Release Date:	28 July 2014

Summary

Multiple OpenSSL vulnerabilities

Recently announced vulnerabilities in OpenSSL allow for possible attacks against the SSL & TLS protocols. These vulnerabilities affect multiple Lexmark products.

References

CVE:

CVE-2014-0224	SSL/TLS MITM vulnerability
CVE-2014-0221	DTLS recursion flaw
CVE-2014-0195	DLTS invalid fragment vulnerability
CVE-2014-0198	SSL_MODE_RELEASE_BUFFERS NULL pointer dereference
CVE-2010-5298	SSL_MODE_RELEASE_BUFFERS session injection of denial of service
CVE-2014-3470	ECDH denial of service
CVE-2014-0076	ECDSA NONCE side channel attack

Details

On June 5, 2014 the OpenSSL Project released a security advisory detailing multiple vulnerabilities. These vulnerabilities include:

CVE-2014-0224 SSL/TLS MITM vulnerability
A remote attacker with the ability to intercept and inject traffic between a vulnerable client and server could successfully force the SSL/TLS protocols to use a known session key, thus rendering the content of those communications vulnerable to interception and modification.

CVSS	Base Score	6.8		(AV:N/AC:M/AU:N/C:P/I:P/A:P)
	Impact Subscore:		6.4	
	Exploitability Subscore:		8.6	

CVE-2014-0221 DTLS recursion flaw
Sending an invalid DTLS handshake can cause a crash leading to a denial of service attack.

NOTE: No Lexmark products support the DTLS protocol; therefore no Lexmark products are vulnerable to this issue.

CVE-2014-0195 DLTS invalid fragment vulnerability
A buffer overrun can be triggered by sending an invalid DTLS fragment.

NOTE: No Lexmark products support the DTLS protocol; therefore no Lexmark products are vulnerable to this issue.

CVE-2014-0198   SSL_MODE_RELEASE_BUFFERS NULL pointer dereference

A remote attacker could send a specially crafted packet that would trigger a crash leading to a denial of service attack.

CVSS	Base Score	4.3		(AV:N/AC:M/AU:N/C:N/I:N/A:P)
	Impact Subscore:		2.9	
	Exploitability Subscore:		8.6	

CVE-2010-5298   SSL_MODE_RELEASE_BUFFERS session injection of denial of service

A remote attacker could send a specially crafted packet that would trigger a crash leading to a denial of service attack.

CVSS	Base Score	4.0		(AV:N/AC:H/AU:N/C:N/I:P/A:P)
	Impact Subscore:		4.9	
	Exploitability Subscore:		4.9	

CVE-2014-3470   ECDH denial of service

A remote attacker could trigger a crash leading to a denial of service attack.

CVSS	Base Score	4.3		(AV:N/AC:M/AU:N/C:N/I:N/A:P)
	Impact Subscore:		2.9	
	Exploitability Subscore:		8.6	

CVE-2014-0076   ECDSA NONCE side channel attack

ECDSA nonce is vulnerable to a timing based side channel attack.

CVSS	Base Score	4.3		(AV:N/AC:M/AU:N/C:PI:N/A:N)
	Impact Subscore:		2.9	
	Exploitability Subscore:		8.6	

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:

- MarkVision Enterprise

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.

- Lexmark printer products
- Perceptive Content: ImageNow
- Perceptive Search
- Perceptive Process
- 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 device 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**
X548 & XS548	**LHS30.VK.P345** and previous	**LHS30.VK.P346** and later
X792 & XS796	LHS30.MR.P345 and previous	LHS30.MR.P346 and later
X925 & XS925	LHS30.HK.P345 and previous	LHS30.HK.P346 and later
X950, X952, X954 & XS955	LHS30.TQ.P345 and previous	LHS30.TQ.P346 and later
6500e	LHS30.JR.P345 and previous	LHS30.JR.P346 and later
CS310	**LW40.VYL.P449** and previous	**LW40.VYL.P450** and later
CS410	LW40.VY2.P449 and previous	LW40.VY2.P450 and later
CS510	LW40.VY4.P449 and previous	LW40.VY4.P450 and later
CX310	LW40.GM2.P449 and previous	LW40.GM2.P450 and later
CX410	LW40.GM4.P449 and previous	LW40.GM4.P450 and later
CX510	LW40.GM7.P449 and previous	LW40.GM7.P450 and later
XC2132	LW40.GM7.P449 and previous	LW40.GM7.P450 and later
MS310	LW40.PRL.P449 and previous	LW40.PRL.P450 and later
MS410	LW40.PRL.P449 and previous	LW40.PRL.P450 and later
MS510	LW40.PR2.P449 and previous	LW40.PR2.P450 and later
MS610dn & MS610dtn	LW40.PR2.P449 and previous	LW40.PR2.P450 and later
M1145 & M3150dn	LW40.PR2.P449 and previous	LW40.PR2.P450 and later
MS610de & MS610dte	LW40.PR4.P449 and previous	LW40.PR4.P450 and later
M3150	LW40.PR4.P449 and previous	LW40.PR4.P450 and later
MS71x	LW40.DN2.P449 and previous	LW40.DN2.P450 and later
MS810n, MS810dn & MS810dtn	LW40.DN2.P449 and previous	LW40.DN2.P450 and later
MS811	LW40.DN2.P449 and previous	LW40.DN2.P450 and later

MS812dn, MS812dtn	LW40.DN2.P449 and previous	LW40.DN2.P450 and later
M5163dn	LW40.DN2.P449 and previous	LW40.DN2.P450 and later
MS810de	LW40.DN4.P449 and previous	LW40.DN4.P450 and later
M5155 & M5163	LW40.DN4.P449 and previous	LW40.DN4.P450 and later
MS812de	LW40.DN7.P449 and previous	LW40.DN7.P450 and later
M5170	LW40.DN7.P449 and previous	LW40.DN7.P450 and later
MX310	LW40.SB2.P449 and previous	LW40.SB2.P450 and later
MX410, MX510 & MX511	LW40.SB4.P449 and previous	LW40.SB4.P450 and later
XM1145	LW40.SB4.P449 and previous	LW40.SB4.P450 and later
MX610 & MX611	LW40.SB7.P449 and previous	LW40.SB7.P450 and later
XM3150	LW40.SB7.P449 and previous	LW40.SB7.P450 and later
MX71x	LW40.TU.P449 and previous	LW40.TU.P450 and later
MX81x	LW40.TU.P449 and previous	LW40.TU.P450 and later
XM51xx & XM71xx	LW40.TU.P449 and previous	LW40.TU.P450 and later
MX6500e	LF40.JD.P449 and previous	Contact **Lexmark Technical Support**.
MS911de	LW40.SA.P448 and previous	LW40.SA.P450 and later
MX91x	LW40.MG.P449 and previous	LW40.MG.P450 and later
X94x	LC.BR.P145 and previous	Contact **Lexmark Technical Support**.
X86x	LP.SP.P692 and previous	LP.SP.P693 and later
X85x	LC4.BE.P488 and previous	Contact **Lexmark Technical Support**.
X782e	LC2.TO.P336 and previous	LC2.TO.P305cS and later
X78x	LC2.IO.P336 and previous	Contact **Lexmark Technical Support**.
X772e	LC.TR.P291 and previous	Contact **Lexmark Technical Support**.
X73x	LR.FL.P691 and previous	LR.FL.P692 and later
X65x	LR.MN.P691 and previous	LR.MN.P692 and later
X644 & X646	LC2.MC.P374 and previous	Contact **Lexmark Technical Support**.
X64xef	LC2.TI.P327 and previous	Contact **Lexmark Technical Support**.
X642	LC2.MB.P318 and previous	Contact **Lexmark Technical Support**.
X546	LL.EL.P544 and previous	Contact **Lexmark Technical Support**.
X543 & X544	LL.EL.P544 and previous	Contact **Lexmark Technical Support**.
X46x	LR.BS.P691 and previous	LR.BS.P692 and later
X36x & X26x	LL.BZ.P544 and previous	Contact **Lexmark Technical Support**.
X20x	LM1.MT.P233 and previous	Contact **Lexmark Technical Support**.
W840	LS.HA.P253 and previous	Contact **Lexmark Technical Support**.
W850	LP.JB.P1644 and previous	Contact **Lexmark Technical Support**.

T656	LSJ.SJ.P039 and previous	Contact **Lexmark Technical Support**.
T650 T652 T654	LR.JP.P677 and previous	Contact **Lexmark Technical Support**.
T64x	LS.ST.P347 and previous	Contact **Lexmark Technical Support**.
N4000	LC.MD.P012d and previous	Contact **Lexmark Technical Support**.
N4050e	GO.GO.N206 and previous	Contact **Lexmark Technical Support**.
N70xxe	LC.CO.N309 and previous	Contact **Lexmark Technical Support**.
N8120 N8130	LR.MU.P311f and previous	Contact **Lexmark Technical Support**.
E462	LR.LBH.P672 and previous	Contact **Lexmark Technical Support**.
E460	LR.LBH.P672 and previous	Contact **Lexmark Technical Support**.
E450	LM.SZ.P124 and previous	Contact **Lexmark Technical Support**.
E360dn	LL.LBM.P539 and previous	Contact **Lexmark Technical Support**.
E260 E360d	LL.LBL.P539 and previous	Contact **Lexmark Technical Support**.
C935dn	LC.JO.P091 and previous	Contact **Lexmark Technical Support**.
C920	LS.TA.P153 and previous	Contact **Lexmark Technical Support**.
C78x	LC.IO.P188 and previous	Contact **Lexmark Technical Support**.
C77x	LC.CM.P053 and previous	Contact **Lexmark Technical Support**.
C73x	LR.SK.P691 and previous	Contact **Lexmark Technical Support**.
C546	LU.AS.P532 and previous	Contact **Lexmark Technical Support**.
C540 C543 C544	LL.AS.P535 and previous	Contact **Lexmark Technical Support**.
C53x	LS.SW.P070 and previous	Contact **Lexmark Technical Support**.
C52x	LS.FA.P151 and previous	Contact **Lexmark Technical Support**.
25xxN	LCL.CU.P114 and previous	Contact **Lexmark Technical Support**.

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

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 4.8.3 or later are not vulnerable, all earlier versions of LDD are vulnerable. A patch is available for the vulnerable versions of LDD that upgrades the OpenSSL library to version 1.0.1h.

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 version 2.3.14.0 (or later) is not vulnerable, but versions 2.3.13 and previous are known to be vulnerable.

Workarounds

Lexmark recommends updating the application 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: 2.27.4.0.31
- Lexmark Fleet Tracker: 2.27.4.0.30

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 Technical Support** at Lexmark Support website, go to your product's support page and locate **Get In Touch with Lexmark!** for contact information.

Perceptive Content

Perceptive Content versions 6.6, 6.7, and 6.8 are vulnerable when using Envoy to make outbound calls with SSL enabled.

Workarounds

Modify the server being called to use a non-vulnerable version of OpenSSL.

Obtaining Updated Software

An update is not currently available. Perceptive Software plans to resolve this vulnerability in a future release.

Perceptive Search

Perceptive Enterprise Search, versions 10.0, 10.1, 10.2, and 10.3 are vulnerable.

Workarounds

Perceptive recommends applying the patch.

Obtaining Updated Software

Perceptive Search 10.x OpenSSL 1.0.1h Patch is available via the Perceptive Software Customer Portal. (www.perceptivesoftware.com) This patch will be included in Perceptive Enterprise Search 10.4.

Perceptive Process

Perceptive Process, versions 2.8, 2.9, 3.0, and 3.1 are vulnerable on the Windows platform. On the UNIX platform Perceptive Process utilizes the OpenSSL libraries that are part of the platform and therefore patching OpenSSL on the platform will address the vulnerability.

Workarounds

There are currently no workarounds.

Obtaining Updated Software

An update is not currently available. Perceptive Software plans to have this rectified in Perceptive Process 3.3.

Exploitation and Public Announcements

Lexmark is not aware of any malicious use 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	18 -July-2014	Initial Release
1.1	21-July-2014	Additional product information added
1.2	19-July-2021	Updated legal notice