Lexmark Security Advisory:

Revision: 1.3
Last update: 19 July 2021
Public Release Date: 4 November 2014

Summary

POODLE (Padding Oracle On Downgraded Legacy Encryption) vulnerability

A vulnerability was disclosed in the SSLv3 protocol which allows an attacker with the ability to intercept and insert traffic (Man-In-The-Middle) to decrypt a portion of the encrypted communication.

References

CVE: CVE-2014-3566

Details

On October 14, 2014, a vulnerability was announced by Google researchers in the way the Secure Sockets Layer version 3 (SSLv3) protocol handles block ciphers in Cipher Block Chaining (CBC) mode. This vulnerability can be exploited by an attacker to decrypt a portion of the encrypted communication, most notably session cookies.

SSLv3 is an old protocol which contains a considerable number of known vulnerabilities. With the addition of this vulnerability use of SSLv3 is now considered insecure; the more modern Transport Layer Security (TLS) protocol should be used in place of SSL..

CVSS	Base Score	4.3		(AV:N/AC:M/AU:N/C:P/I: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

This vulnerability can be used to expose a portion of SSLv3 protected communications. This information can include session cookies which can then be leveraged to obtain unauthorized access.

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
- Markvision Enterprise

Additional products may be affected, investigations are ongoing.

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 a devices firmware level, select the “Reports”->”Menu Setting Page” menu item from the operator panel. If the firmware level listed under “Device Information” matches any level under “Affected Releases”, then upgrade to a “Fixed Release”.

Additional products may be affected, investigations are ongoing.

Lexmark Models	Affected Releases	Fixed Releases
CS31x	LW41.VYL.P468 and previous	LW41.VYL.P469 and later
CS41x	LW41.VY2.P468 and previous	LW41.VY2.P469 and later
CS51x	LW41.VY4.P468 and previous	LW41.VY4.P469 and later
CX310	LW41.GM2.P468 and previous	LW41.GM2.P469 and later
CX410	LW41.GM4.P468 and previous	LW41.GM4.P469 and later
CX510	LW41.GM7.P468 and previous	LW41.GM7.P469 and later
XC2132	LW41.GM7.P468 and previous	LW41.GM7.P469 and later
MS310	LW41.PRL.P468 and previous	LW41.PRL.P469 and later
MS312	LW41.PRL.P468 and previous	LW41.PRL.P469 and later
MS315	LW41.TL.P468 and previous	LW41.TL.P469 and later
MS410	LW41.PRL.P468 and previous	LW41.PRL.P469 and later
MS415	LW41.TL.P468 and previous	LW41.TL.P469 and later
MS51x	LW41.PR2.P468 and previous	LW41.PR2.P469 and later
MS610dn & MS610dtn	LW41.PR2.P468 and previous	LW41.PR2.P469 and later
M1145 & M3150dn	LW41.PR2.P468 and previous	LW41.PR2.P469 and later
MS610de & MS610dte	LW41.PR4.P468 and previous	LW41.PR4.P469 and later
M3150	LW41.PR4.P468 and previous	LW41.PR4.P469 and later
MS71x	LW41.DN2.P468 and previous	LW41.DN2.P469 and later
MS810n, MS810dn & MS810dtn	LW41.DN2.P468 and previous	LW41.DN2.P469 and later
MS811	LW41.DN2.P468 and previous	LW41.DN2.P469 and later
MS812dn, MS812dtn	LW41.DN2.P468 and previous	LW41.DN2.P469 and later
M5163dn	LW41.DN2.P468 and previous	LW41.DN2.P469 and later
MS810de	LW41.DN4.P468 and previous	LW41.DN4.P469 and later
M5155 & M5163	LW41.DN4.P468 and previous	LW41.DN4.P469 and later
MS812de	LW41.DN7.P468 and previous	LW41.DN7.P469 and later
M5170	LW41.DN7.P468 and previous	LW41.DN7.P469 and later
MS91x	LW41.SA.P468 and previous	LW41.SA.P469 and later
MX310	LW41.SB2.P468 and previous	LW41.SB2.P469 and later
MX410, MX510 & MX511	LW41.SB4.P468 and previous	LW41.SB4.P469 and later
XM1145	LW41.SB4.P468 and previous	LW41.SB4.P469 and later
MX610 & MX611	LW41.SB7.P468 and previous	LW41.SB7.P469 and later
XM3150	LW41.SB7.P468 and previous	LW41.SB7.P469 and later
MX71x	LW41.TU.P468 and previous	LW41.TU.P469 and later
MX81x	LW41.TU.P468 and previous	LW41.TU.P469 and later
XM51xx & XM71xx	LW41.TU.P468 and previous	LW41.TU.P469 and later

MX91x	LW41.MG.P468 and previous	LW41.MG.469 and later
MX6500e	LW41.JD.P468 and previous	LW41.JD.P469 and later
C746	LHS41.CM2.P458 and previous	LHS41.CM2.P459 and later
C748 & CS748	LHS41.CM4.P458 and previous	LHS41.CM4.P459 and later
C79x & CS796	LHS41.HC.P458 and previous	LHS41.HC.P459 and later
C925	LHS41.HV.P458 and previous	LHS41.HV.P459 and later
C95x	LHS41.TP.P458 and previous	LHS41.TP.P459 and later
X548 & XS548	LHS41.VK.P458 and previous	LHS41.VK.P459 and later
X74x & XS748	LHS41.NY.P458 and previous	LHS41.NY.P459 and later
X792 & XS79x	LHS41.MR.P458 and previous	LHS41.MR.P459 and later
X925 & XS925	LHS41.HK.P458 and previous	LHS41.HK.P459 and later
X95x & XS95x	LHS41.TQ.P458 and previous	LHS41.TQ.P459 and later
6500e	LHS41.JR.P458 and previous	LHS41.JR.P459 and later
C734	LR.SK.P693 and previous	LR.SK.P694 and later
E46x	LR.LBH.P673 and previous	LR.LBH.P674 and later
T650 & T652	LR.JP.P680 and previous	LR.JP.P681 and later
T654	LR.JP.P680 and previous	LR.JP.P681 and later
T656	LSJ.SJ.P041 and previous	LSJ.SJ.P042 and later
W85x	LR.JB.P645 and previous	LR.JB.P646 and later
X46x	LR.BS.P695 and previous	LR.BS.P696 and later
X65x	LR.MN.P694 and previous	LR.MN.P695 and later
X73x	LR.FL.P694 and previous	LR.FL.P695 and later
X86x	LP.SP.P694 and previous	LP.SP.P695 and later

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.

Markvision Enterprise

The vulnerability has been fixed in Markvision Enterprise v2.1 and all future releases. All releases previous to v2.1 are vulnerable.

Obtaining Updated Software

To obtain Markvision Enterprise v2.1, please visit http://www.lexmark.com/markvision.

Workarounds

The vulnerability only exists when SSLv3 is in use. Therefore Lexmark recommends that you disable SSLv3 support in your browser and other applications. Contact your application provider for information on how to accomplish this.

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

Revision	Date	Reason
1.0	3-November-2014	Initial Public Release
1.1	12-November-2014	Updated to identify affected products
1.2	25-November-2014	Updated to identify additional affected products
1.3	19-July-2021	Updated legal notice