Lexmark Security Advisory:

Revision: 1.0
Last update: 30 June 2015
Public Release Date: 7 July 2015

Summary

Logjam: Weaknesses in SSL/TLS Diffie-Hellman key exchange.

Two vulnerabilities were discovered in how many SSL/TLS implementations handle Diffie-Hellman (DH) key exchange. The first vulnerability allows a Man-In-The-Middle attacker to downgrade vulnerable SSL/TLS connections to 512 bit (weak) cryptography. The second vulnerability is the fact that many SSL/TLS implementations use the same prime numbers in their Diffie-Hellman key exchange leaving them vulnerable to a pre-computation attack.

References

CVE: CVE-2015-4000

Details

On May 20th 2015 vulnerabilities were announced in how many SSL/TLS implementations handle Diffie-Hellman (DH) key exchange. The vulnerabilities are:

1. Some vulnerable implementations of the SSL/TLS protocol allow a Man-In-The-Middle attacker to manipulate the SSL/TLS handshake when a Diffie-Hellman cipher is selected to force the use of a weak 512 bit prime. The weak prime can then be exploited to compromise the security of the SSL/TLS connection.
2. Many implementations of the SSL/TLS protocol use the same prime numbers when performing Diffie-Hellman negotiations. This allows an attacker to pre-compute tables that greatly simplify the process of compromising connections established with those known primes.

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

Successful exploitation of this vulnerability can lead to the disclosure and/or modification of information traveling over the affected SSL/TLS communication channel.

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

Product Specific Information

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

Laser printer products

NOTE: *None of Lexmark's printer products have network services that support the use of Diffie-Hellman and therefore none of these services are vulnerable. However these products when communicating with a SSL/TLS server do support Diffie-Hellman and allow the selection of a weak prime. As documented below, these products have been modified to no longer accept a weak prime.*

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".

Lexmark Models	**Affected Releases**	**Fixed Releases**
CS31x	LW50.VYL.P554 and previous	LW50.VYL.P555 and later
CS41x	LW50.VY2.P554 and previous	LW50.VY2.P555 and later
CS51x	LW50.VY4.P554 and previous	LW50.VY4.P555 and later
CX310	LW50.GM2.P554 and previous	LW50.GM2.P555 and later
CX410	LW50.GM4.P554 and previous	LW50.GM4.P555 and later
CX510	LW50.GM7.P554 and previous	LW50.GM7.P555 and later
XC2132	LW50.GM7.P554 and previous	LW50.GM7.P555 and later
MS310	LW50.PRL.P554 and previous	LW50.PRL.P555 and later
MS312	LW50.PRL.P554 and previous	LW50.PRL.P555 and later
MS315	LW50.TL2.P554 and previous	LW50.TL2.P555 and later
MS410	LW50.PRL.P554 and previous	LW50.PRL.P555 and later
MS415	LW50.TL2.P554 and previous	LW50.TL2.P555 and later
MS51x	LW50.PR2.P554 and previous	LW50.PR2.P555 and later
MS610dn & MS610dtn	LW50.PR2.P554 and previous	LW50.PR2.P555 and later
M1145 & M3150dn	LW50.PR2.P554 and previous	LW50.PR2.P555 and later
MS610de & MS610dte	LW50.PR4.P554 and previous	LW50.PR4.P555 and later
M3150	LW50.PR4.P554 and previous	LW50.PR4.P555 and later
MS71x	LW50.DN2.P554 and previous	LW50.DN2.P555 and later
MS810n, MS810dn & MS810dtn	LW50.DN2.P554 and previous	LW50.DN2.P555 and later
MS811	LW50.DN2.P554 and previous	LW50.DN2.P555 and later
MS812dn, MS812dtn	LW50.DN2.P554 and previous	LW50.DN2.P555 and later
M5163dn	LW50.DN2.P554 and previous	LW50.DN2.P555 and later
MS810de	LW50.DN4.P554 and previous	LW50.DN4.P555 and later
M5155 & M5163	LW50.DN4.P554 and previous	LW50.DN4.P555 and later
MS812de	LW50.DN7.P554 and previous	LW50.DN7.P555 and later
M5170	LW50.DN7.P554 and previous	LW50.DN7.P555 and later
MS91x	LW50.SA.P554 and previous	LW50.SA.P555 and later
MX310	LW50.SB2.P554 and previous	LW50.SB2.P555 and later
MX410, MX510 & MX511	LW50.SB4.P554 and previous	LW50.SB4.P555 and later

XM1145	LW50.SB4.P554 and previous	LW50.SB4.P555 and later
MX610 & MX611	LW50.SB7.P554 and previous	LW50.SB7.P555 and later
XM3150	LW50.SB7.P554 and previous	LW50.SB7.P555 and later
MX71x	LW50.TU.P554 and previous	LW50.TU.P555 and later
MX81x	LW50.TU.P554 and previous	LW50.TU.P555 and later
XM51xx & XM71xx	LW50.TU.P554 and previous	LW50.TU.P555 and later
MX91x	LW50.MG.P554 and previous	LW50.MG.555 and later
MX6500e	LW50.JD.P554 and previous	LW50.JD.555 and later
C746	LHS41.CM2.P487 and previous	LHS41.CM2.P488 and later
C748 & CS748	LHS41.CM4.P487 and previous	LHS41.CM4.P488 and later
C79x & CS796	LHS41.HC.P487 and previous	LHS41.HC.P488 and later
C925	LHS41.HV.P487 and previous	LHS41.HV.P488 and later
C95x	LHS41.TP.P487 and previous	LHS41.TP.P488 and later
X548 & XS548	LHS41.VK.P487 and previous	LHS41.VK.P488 and later
X74x & XS748	LHS41.NY.P487 and previous	LHS41.NY.P488 and later
X792 & XS79x	LHS41.MR.P487 and previous	LHS41.MR.P488 and later
X925 & XS925	LHS41.HK.P487 and previous	LHS41.HK.P488 and later
X95x & XS95x	LHS41.TQ.P487 and previous	LHS41.TQ.P488 and later
6500e	LHS41.JR.P487 and previous	LHS41.JR.P488 and later
C734	LR.SK.P697 and previous	LR.SK.P698 and later
C736	LR.SKE.P695 and previous	LR.SKE.P696 and later
E46x	LR.LBH.P677 and previous	LR.LBH.P678 and later
T650 & T652	LR.JP.P685 and previous	LR.JP.P686 and later
T654	LR.JP.P685 and previous	LR.JP.P686 and later
T656	LSJ.SJ.P045 and previous	LSJ.SJ.P046 and later
W85x	LR.JB.P648 and previous	LR.JB.P649 and later
X46x	LR.BS.P701 and previous	LR.BS.P702 and later
X65x	LR.MN.P702 and previous	LR.MN.P703 and later
X73x	LR.FL.P700 and previous	LR.FL.P701 and later
X86x	LP.SP.P701 and previous	LP.SP.P702 and later
C54x	Not Vulnerable	Not Vulnerable
E26x	Not Vulnerable	Not Vulnerable
E36x	Not Vulnerable	Not Vulnerable
X26x	Not Vulnerable	Not Vulnerable
X36x	Not Vulnerable	Not Vulnerable
X54x	Not Vulnerable	Not Vulnerable
C52x	In Evaluation	Contact Lexmark
C53x	In Evaluation	Contact Lexmark
C77x	In Evaluation	Contact Lexmark
C78x	In Evaluation	Contact Lexmark
C92x	In Evaluation	Contact Lexmark
C93x	In Evaluation	Contact Lexmark
E45x	In Evaluation	Contact Lexmark
T64x	In Evaluation	Contact Lexmark
W84x	In Evaluation	Contact Lexmark
X642	In Evaluation	Contact Lexmark
X644/X646	In Evaluation	Contact Lexmark
X64xef	In Evaluation	Contact Lexmark
X85x	In Evaluation	Contact Lexmark
X94x	In Evaluation	Contact Lexmark

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 updating firmware to address this issue.

Exploitation and Public Announcements

Lexmark is not aware of any malicious use against Lexmark products 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	7-July-2015	Initial Public Release