Lexmark Security Advisory:

Revision: 1.1
Last update: 23 July 2021
Public Release Date: 20 April 2015

Summary

FREAK: (Factoring Attack on RSA-EXPORT Keys) vulnerability

A vulnerability was disclosed in some implementations of the SSL/TLS protocol that allow an attacker to downgrade the encryption used by the protocol.

References

CVE: CVE-2015-0204, CVE-2015-1637

Details

A SSL/TLS protocol vulnerability, nicknamed FREAK, has been identified that allows a MITM (Main In The Middle) attacker to force the significant downgrade of the encryption used to protect the SSL/TLS communication. Many SSL/TLS implementations are affected including both OpenSSL and MS Schannel.

CVSS	Base Score	7.8	(AV:N/AC:L/AU:N/C:C/I:N/A:N)
	Impact Subscore:	6.9	
	Exploitability Subscore:	10	

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

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	LW41.VYL.P486 and previous	LW41.VYL.P487 and later
CS41x	LW41.VY2.P486 and previous	LW41.VY2.P487 and later
CS51x	LW41.VY4.P486 and previous	LW41.VY4.P487 and later
CX310	LW41.GM2.P486 and previous	LW41.GM2.P487 and later
CX410	LW41.GM4.P486 and previous	LW41.GM4.P487 and later
CX510	LW41.GM7.P486 and previous	LW41.GM7.P487 and later
XC2132	LW41.GM7.P486 and previous	LW41.GM7.P487 and later
MS310	LW41.PRL.P4816and previous	LW41.PRL.P487 and later
MS312	LW41.PRL.P4816and previous	LW41.PRL.P487 and later
MS315	LW41.TL2.P486 and previous	LW41.TL2.P487 and later
MS410	LW41.PRL.P486 and previous	LW41.PRL.P487 and later
MS415	LW41.TL2.P486 and previous	LW41.TL2.P487 and later
MS51x	LW41.PR2.P486 and previous	LW41.PR2.P487 and later
MS610dn & MS610dtn	LW41.PR2.P486 and previous	LW41.PR2.P487 and later
M1145 & M3150dn	LW41.PR2.P486 and previous	LW41.PR2.P487 and later
MS610de & MS610dte	LW41.PR4.P486 and previous	LW41.PR4.P487 and later
M3150	LW41.PR4.P486 and previous	LW41.PR4.P487 and later
MS71x	LW41.DN2.P486 and previous	LW41.DN2.P487 and later
MS810n, MS810dn & MS810dtn	LW41.DN2.P486 and previous	LW41.DN2.P487 and later
MS811	LW41.DN2.P486 and previous	LW41.DN2.P487 and later
MS812dn, MS812dtn	LW41.DN2.P486 and previous	LW41.DN2.P487 and later
M5163dn	LW41.DN2.P486 and previous	LW41.DN2.P487 and later
MS810de	LW41.DN4.P486 and previous	LW41.DN4.P487 and later
M5155 & M5163	LW41.DN4.P486 and previous	LW41.DN4.P487 and later
MS812de	LW41.DN7.P486 and previous	LW41.DN7.P487 and later
M5170	LW41.DN7.P486 and previous	LW41.DN7.P487 and later
MS91x	LW41.SA.P486 and previous	LW41.SA.P487 and later
MX310	LW41.SB2.P486 and previous	LW41.SB2.P487 and later
MX410, MX510 & MX511	LW41.SB4.P486 and previous	LW41.SB4.P487 and later
XM1145	LW41.SB4.P486 and previous	LW41.SB4.P487 and later
MX610 & MX611	LW41.SB7.P486 and previous	LW41.SB7.P487 and later
XM3150	LW41.SB7.P486 and previous	LW41.SB7.P487 and later
MX71x	LW41.TU.P486 and previous	LW41.TU.P487 and later
MX81x	LW41.TU.P486 and previous	LW41.TU.P487 and later
XM51xx & XM71xx	LW41.TU.P486 and previous	LW41.TU.P487 and later
MX91x	LW41.MG.P486 and previous	LW41.MG.487 and later
MX6500e	LW41.JD.P486 and previous	LW41.JD.487 and later
C746	LHS41.CM2.P476 and previous	LHS41.CM2.P477 and later
C748 & CS748	LHS41.CM4.P476 and previous	LHS41.CM4.P477 and later
C79x & CS796	LHS41.HC.P476 and previous	LHS41.HC.P477 and later
C925	LHS41.HV.P476 and previous	LHS41.HV.P477 and later
C95x	LHS41.TP.P476 and previous	LHS41.TP.P477 and later

X548 & XS548	LHS41.VK.P476 and previous	LHS41.VK.P477 and later
X74x & XS748	LHS41.NY.P476 and previous	LHS41.NY.P477 and later
X792 & XS79x	LHS41.MR.P476 and previous	LHS41.MR.P477 and later
X925 & XS925	LHS41.HK.P476 and previous	LHS41.HK.P477 and later
X95x & XS95x	LHS41.TQ.P476 and previous	LHS41.TQ.P477 and later
6500e	LHS41.JR.P476 and previous	LHS41.JR.P477 and later
C734	LR.SK.P696 and previous	LR.SK.P697 and later
C736	LR.SKE.P694 and previous	LR.SKE.P695 and later
E46x	LR.LBH.P675 and previous	LR.LBH.P676 and later
T650 & T652	LR.JP.P684 and previous	LR.JP.P685 and later
T654	LR.JP.P684 and previous	LR.JP.P685 and later
T656	LSJ.SJ.P044 and previous	LSJ.SJ.P045 and later
W85x	LR.JB.P647 and previous	LR.JB.P648 and later
X46x	LR.BS.P698 and previous	LR.BS.P699 and later
X65x	LR.MN.P700 and previous	LR.MN.P701 and later
X73x	LR.FL.P698 and previous	LR.FL.P699 and later
X86x	LP.SP.P700 and previous	LP.SP.P701 and later
C54x	LL.AS.P536 and previous	LL.AS.P537 and later
E26x	LL.LBL.P541 and previous	LL.LBL.P542 and later
E36x	LL.LBM.P541 and previous	LL.LBM.P542 and later
X26x	LL.BZ.P546 and previous	LL.BZ.P547 and later
X36x	LL.BZ.P546 and previous	LL.BZ.P547 and later
X54x	LL.EL.P546 and previous	LL.EL.P547 and later
C52x	LS.FA.P152 and previous	LS.FA.P153 and later
C53x	LS.SW.P071 and previous	LS.SW.P072 and later
C77x	LC.CM.P503 and previous	LC.CM.P054 and later
C78x	LC.IO.P190 and previous	LC.IO.P190 and later
C92x	LS.TA.P154 and previous	LS.TA.P155 and later
C93x	LC.JO.P095 and previous	LC.JO.P096 and later
E45x	LM.SZ.P124 and previous	LM.SZ.P125 and later
T64x	LS.ST.P353 and previous	LS.ST.P354 and later
W84x	LS.HA.P254 and previous	LS.HA.P255 and later
X642	LC2.MB.P318 and previous	LC2.MB.P319 and later
X644/X646	LC2.MC.P377 and previous	LC2.MC.P378 and later
X64xef	LC2.TI.P329 and previous	LC2.TI.P330 and later
X77x	LC2.TR.P291 and previous	LC2.TR.P292 and later
X78x	LC2.TO.P339 and previous	LC2.TO.P340 and later
X85x	LC4.BE.P491 and previous	LC4.BE.P492 and later
X94x	LC.BR.P153 and previous	LC.BR.P154 and later
N4000	LC.MD.P119 and previous	Contact Lexmark
N4050e	GO.GO.N206 and previous	Contact Lexmark
N7xxe	LC.CO.N309 and previous	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	20-April-2015	Initial Public Release
1.1	23-July-2021	Updated legal notice