Lexmark Security Advisory:

Revision: 1.0
Last update: 12 March 2018
Public Release Date: 12 March 2018

Summary

Lexmark has learned of a series of weaknesses in WPA2, the protocol that secures all modern protected Wi-Fi networks. The weaknesses are in the WPA2 standard itself, and therefore many implementations of WPA2 protocol are likely affected.

Some Lexmark products support Wi-Fi.
Multiple Lexmark products are affected by this vulnerability when Wi-Fi is enabled.

References

CVEs:

- CVE-2017-13077
- CVE-2017-13078
- CVE-2017-13079
- CVE-2017-13080
- CVE-2017-13081
- CVE-2017-13082
- CVE-2017-13084
- CVE-2017-13086
- CVE-2017-13087
- CVE-2017-13088

Details

CVE-2017-13077

A vulnerability in the processing of the 802.11i 4-way handshake messages of the WPA and WPA2 protocols could allow an unauthenticated, or malicious attacker to force a reinstall of a previously used pairwise key.

CVSS v3 Base Score:	6.8	(AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)
Impact Score:	5.2	
Exploitability Score:	1.6	

CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss/user-guide)

CVE-2017-13078

A vulnerability in the processing of the 802.11i 4-way handshake messages of the WPA and WPA2 protocols could allow an unauthenticated, or malicious attacker to force a reinstall of a previously used group key.

CVSS v3 Base Score: 5.3 ((AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

Impact Score: 3.6

Exploitability Score: 1.6

CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss/user-guide)

CVE-2017-13079

A vulnerability in the processing of the 802.11i 4-way handshake messages of the WPA and WPA2 protocols could allow an unauthenticated, or malicious attacker to force a reinstall of a previously used integrity group key.

CVSS v3 Base Score: 5.3 (AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

Impact Score: 3.6

Exploitability Score: 1.6

CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss/user-guide)

CVE-2017-13080

A vulnerability in the processing of the 802.11i group key handshake messages of the WPA and WPA2 protocols could allow an unauthenticated, or malicious attacker to force a reinstall of a previously used group key.

CVSS v3 Base Score: 5.3 (AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

Impact Score: 3.6

Exploitability Score: 1.6

CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss/user-guide)

CVE-2017-13081

A vulnerability in the processing of the 802.11i group key handshake messages of the WPA and WPA2 protocols could allow an unauthenticated, or malicious attacker to force a reinstall of a previously used integrity group key.

CVSS v3 Base Score: 5.3 (AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

Impact Score: 3.6

Exploitability Score: 1.6

CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss/user-guide)

CVE-2017-13082

A vulnerability in the processing of the 802.11r Fast BSS (Basic Service Set) Transition handshake messages of the WPA and WPA2 protocols could allow an unauthenticated, or malicious attacker to force a reinstall of a previously used pairwise key.

CVSS v3 Base Score: 8.1 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)

Impact Score: 5.2

Exploitability Score: 2.8

CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss/user-guide)

CVE-2017-13084

A vulnerability in the processing of the 802.11 PeerKey handshake messages of the WPA and WPA2 protocols could allow an unauthenticated, adjacent attacker to force an station-to-station link (STSL) to reinstall a previously used station-to-station link Transient Key (STK).

CVSS v3 Base Score:	6.8	(AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)
Impact Score:	5.2	
Exploitability Score:	1.6	

CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss/user-guide)

CVE-2017-13086

A vulnerability in the processing of the 802.11z (Extensions to Direct-Link Setup) Tunneled Direct-Link Setup (TDLS) handshake messages could allow an unauthenticated, adjacent attacker to force a supplicant that is compliant with the 802.11z standard to reinstall a previously used Tunneled Direct-Link Setup PeerKey (TPK) key.

CVSS v3 Base Score:	6.8	(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Impact Score:	5.2	
Exploitability Score:	1.6	

CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss/user-guide)

CVE-2017-13087

A vulnerability in the processing of the 802.11v (Wireless Network Management) Sleep Mode Response frames could allow an unauthenticated, adjacent attacker to force a supplicant that is compliant with the 802.11v standard to reinstall a previously used group key.

CVSS v3 Base Score:	5.3	(AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)
Impact Score:	3.6	
Exploitability Score:	1.6	

CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss/user-guide)

CVE-2017-13088

A vulnerability in the processing of the 802.11v (Wireless Network Management) Sleep Mode Response frames could allow an unauthenticated, adjacent attacker to force a supplicant that is compliant with the 802.11v standard to reinstall a previously used integrity group key.

CVSS v3 Base Score:	5.3	(AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)
Impact Score:	3.6	
Exploitability Score:	1.6	

CVSSv3 scores are calculated in accordance with CVSS version 3.0(https://www.first.org/cvss/user-guide)

Impact

This vulnerability can allow the disclosure of information that was previously assumed to be safely encrypted. This may include sensitive information such as print data, passwords, and so on.

Affected Products

Some Lexmark products support Wi-Fi, and are affected by this vulnerability when Wi-Fi is enabled. The complete list of affected devices is shown below.

To determine a devices firmware level, select the "**Settings**" > "**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 you should upgrade to a "**Fixed Release**".

Lexmark Models	**Affected Releases**	**Fixed Releases**
CX820de, CX820dtfe	CXTPP.041.212 and previous	CXTPP.041.213 and later
XC6152de, XC6152dtfe	CXTPP.041.212 and previous	CXTPP.041.213 and later
CX825de, CX825dte, CX825dtfe	CXTPP.041.212 and previous	CXTPP.041.213 and later
XC8155de, XC8155dte	CXTPP.041.212 and previous	CXTPP.041.213 and later
CX860de, CX860dte, CX860dtfe	CXTPP.041.212 and previous	CXTPP.041.213 and later
XC8160de, XC8160dte	CXTPP.041.212 and previous	CXTPP.041.213 and later
CS820de, CS820dte, CS820dtfe	CSTPP.041.212 and previous	CSTPP.041.213 and later
C6160	CSTPP.041.212 and previous	CSTPP.041.213 and later
CS720de, CS720dte	CSTAT.041.212 and previous	CSTAT.041.213 and later
CS725de, CS725dte	CSTAT.041.212 and previous	CSTAT.041.213 and later
C4150	CSTAT.041.212 and previous	CSTAT.041.213 and later
CX725de, CX725dhe, CX725dthe	CXTAT.041.212 and previous	CXTAT.041.213 and later
XC4150	CXTAT.041.212 and previous	CXTAT.041.213 and later
CS31x	LW63.VYL.P743 and previous	LW63.VYL.P744 and later
CS41x	LW63.VY2.P743 and previous	LW63.VY2.P744 and later
CS51x	LW63.VY4.P743 and previous	LW63.VY4.P744 and later
CX310	LW63.GM2.P743 and previous	LW63.GM2.P744 and later
CX410	LW63.GM4.P743 and previous	LW63.GM4.P744 and later
CX510	LW63.GM7.P743 and previous	LW63.GM7.P744 and later
XC2132	LW63.GM7.P743 and previous	LW63.GM7.P744 and later
MS310	LW63.PRL.P743 and previous	LW63.PRL.P744 and later
MS312	LW63.PRL.P743 and previous	LW63.PRL.P744 and later
MS315	LW63.TL2.P743 and previous	LW63.TL2.P744 and later

MS410	LW63.PRL.P743 and previous	LW63.PRL.P744 and later
MS415	LW63.TL2.P743 and previous	LW63.TL2.P744 and later
MS51x	LW63.PR2.P743 and previous	LW63.PR2.P744 and later
MS610dn & MS610dtn	LW63.PR2.P743 and previous	LW63.PR2.P744 and later
M1145 & M3150dn	LW63.PR2.P743 and previous	LW63.PR2.P744 and later
MS610de & MS610dte	LW63.PR4.P743 and previous	LW63.PR4.P744 and later
M3150	LW63.PR4.P743 and previous	LW63.PR4.P744 and later
MS71x	LW63.DN2.P743 and previous	LW63.DN2.P744 and later
MS810n, MS810dn & MS810dtn	LW63.DN2.P743 and previous	LW63.DN2.P744 and later
MS811	LW63.DN2.P743 and previous	LW63.DN2.P744 and later
MS812dn, MS812dtn	LW63.DN2.P743 and previous	LW63.DN2.P744 and later
M5163dn	LW63.DN2.P743 and previous	LW63.DN2.P744 and later
MS810de	LW63.DN4.P743 and previous	LW63.DN4.P744 and later
M5155 & M5163	LW63.DN4.P743 and previous	LW63.DN4.P744 and later
MS812de	LW63.DN7.P743 and previous	LW63.DN7.P744 and later
M5170	LW63.DN7.P743 and previous	LW63.DN7.P744 and later
MS91x	LW63.SA.P743 and previous	LW63.SA.P744 and later
MX310	LW63.SB2.P743 and previous	LW63.SB2.P744 and later
XM1145	LW63.SB4.P743 and previous	LW63.SB4.P744 and later
MX610 & MX611	LW63.SB7.P743 and previous	LW63.SB7.P744 and later
XM3150	LW63.SB7.P743 and previous	LW63.SB7.P744 and later
MX71x	LW63.TU.P743 and previous	LW63.TU.P744 and later
MX81x	LW63.TU.P743 and previous	LW63.TU.P744 and later
XM51xx & XM71xx	LW63.TU.P743 and previous	LW63.TU.P744 and later
MX91x	LW63.MG.P743 and previous	LW63.MG.P744 and later
MX6500	LW63.JD.P743 and previous	LW63.JD.P744 and later
C746	LHS60.CM2.P647 and previous	LHS60.CM2.P648 and later
C748 & CS748	LHS60.CM4.P647 and previous	LHS60.CM4.P648 and later
C79x & CS796	LHS60.HC.P647 and previous	LHS60.HC.P648 and later
C925	LHS60.HV.P647 and previous	LHS60.HV.P648 and later

C95x	LHS60.TP.P647 and previous	LHS60.TP.P648 and later
X548 & XS548	LHS60.VK.P647 and previous	LHS60.VK.P648 and later
X74x & XS748	LHS60.NY.P647 and previous	LHS60.NY.P648 and later
X792 & XS79x	LHS60.MR.P647 and previous	LHS60.MR.P648 and later
X925 & XS925	LHS60.HK.P647 and previous	LHS60.HK.P648 and later
X95x & XS95x	LHS60.TQ.P647 and previous	LHS60.TQ.P648 and later
6500	LHS60.JR.P647 and previous	LHS60.JR.P648 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.

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.

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	12 March 2018	Initial Public Release