Lexmark Security Advisory:

Revision: 1.1
Last update: 19 July 2021
Public Release Date: 26 Apr 2010

Summary

SSL Denial of service vulnerability.

Some Lexmark Printers and MarkNet Devices contain a denial of service vulnerability in their SSL/TLS processing. This vulnerability can be exploited to crash the printer.

References

CVE: CVE-2004-0079

Affected Products

Older Lexmark Laser printer products and MarkNet devices; for specific details see “Software Versions & Fixes” below.

Details

Secure Socket Layer (SSL) and Transport Layer Security (TLS) can be used to encrypt network communication with the embedded web server (TCP port 443) running on Lexmark products. A carefully crafted SSL/TLS handshake sent to a vulnerable device will cause it to crash.

Impact

Successful exploitation of this vulnerability can lead to a denial of service on the affected printer by causing it to crash.

Vulnerability Scoring Details

CVSS Base Score 5.0

Exploitability:		Impact:	
Access Vector:	Network	Confidentiality:	None
Access Complexity:	Low	Integrity:	None
Authentication:	None	Availability:	Partial

CVSS scores are calculated in accordance with CVSS version 2.0

Software Versions and Fixes

Updated software that removes the vulnerability described in this advisory is available for the following devices:

Lexmark Models	Affected Releases	Fixed Releases
X94x	Base: LC.BR.P051HDs and previous	Base: LC.BR.P051HDs1

	Net: NC.NPS.N129S and previous	Net: NC.NPS.N129S1
X85x	Base: LC4.BE.P457S and previous Net: NC2.NPS.N222S and previous	Base: LC4.BE.P457S1 Net: NC2.NPS.N222S1
X782e	Base: LC2.TO.P305cS and previous Net: NC2.NPS.N222S and previous	Base: LC2.TO.P305cS1 Net: NC2.NPS.N222S1
X772e	Base: LC.TR.P275S and previous Net: NC2.NPS.N222S and previous	Base: LC2.TR.P275S1 Net: NC2.NPS.N222S1
X644 & X646	Base: LC2.MC.P307aS and previous Net: NC2.NPS.N222S and previous	Base: LC2.MC.P307aS1 Net: NC2.NPS.N222S1
X64xef	Base: LC2.TI.P305aS and previous Net: NC2.NPS.N222S and previous	Base: LC2.TI.P305aS1 Net: NC2.NPS.N222S1
X642	Base: LC2.MB.P307bS and previous Net: NC2.NPS.N222S and previous	Base: LC2.MB.P307bS1 Net: NC2.NPS.N222S1
W840	Base: LS.HA.P121S and previous Net: NS.NP.N118S previous	Base: LS.HA.P121S1 Net: NS.NP.N118S1
T64x	Base: LS.ST.P240S and previous Net: NS.NP.N219S and previous	Base: LS.ST.P240S1 Net: NS.NP.N219S1
N70xxe	Net: LC.CO.N069 and previous	Net: LC.CO.N070
C935dn	Base: LC.JO.P051S and previous Net: NC.NPS.N129S and previous	Base: LC.JO.P051S1 Net: NC.NPS.N129S1
C920	Base: LS.TA.P127S and previous Net: NS.NP.N219S and previous	Base: LS.TA.P127S1 Net: NS.NP.N219S1
C78x	Base: LC.IO.P165aS and previous Net: NC2.NPS.N222S and previous	Base: LC.IO.P165aS1 Net: NC2.NPS.N222S1
C77x	Base: LC.CM.P027bS and previous Net. NCC.NPS.N107S1 and previous	Base: LC.CM.P027bS1 Net: NCC.NPS.N107S1
C53x	Base: LS.SW.P026avcS and previous Net: NSF.NP.N026S and previous	Base: LS.SW.P026avcS1 Net: NSF.NP.N026S1
C52x	LS.FA.P129S and previous Net: NS.NP.N219S and previous	Base: LS.FA.P129S1 Net: NS.NP.N219S1
25xxN	Base: LCL.CU.P106 and previous Net: NCL.NA.N105 and previous	Base: LC.CU.P107 Net: NCL.NA.N106

IPDS DLE Versions and Fixes

Lexmark Models	**Fixed Releases**
X94x	Base: LC.BR.P051HDs1 Net: NC.NPS.N129S1
X85x	Base: LC4.BE.P457S1 Net: NC2.NPS.N222S1
X782e	Base: LC2.TO.P305cS1 Net: NC2.NPS.N222S1
X644 & X646	Base: LC2.MC.P307aS1 Net: NC2.NPS.N222S1
X64xef	Base: LC2.TI.P305aS1 Net: NC2.NPS.N222S1
W840	Base: LS.HA.P225S Net: NS.NP.N259*

T64x	Base: LS.ST.P240S1 Net: NS.NP.N219S1
C935dn	Base: LC.JO.P051S1 Net: NC.NPS.N129S1
C920	Base: LS.TA.P127EPs Net: NS.NP.N219S1
C78x	Base: LC.IO.P165aS1 Net: NC2.NPS.N222S1
C77x	Base: LC.CM.P027bS1 Net: NCC.NPS.N107S1

*A network firmware update is required AFTER the base has been updated for this device.

Forms DLE Versions and Fixes

Updated software that removes the vulnerability described in this advisory is available for the following devices:

Lexmark Models	**Fixed Releases**
X94x	Base: LC.BR.P051HDs1 Net: NC.NPS.N129S1
X85x	Base: LC4.BE.P457S1 Net: NC2.NPS.N222S1
X782e	Base: LC2.TO.P305cS1 Net: NC2.NPS.N222S1
X644 & X646	Base: LC2.MC.P307aS1 Net: NC2.NPS.N222S1
X64xef	Base: LC2.TI.P305aS1 Net: NC2.NPS.N222S1
X642	Base: LC2.MB.P307bS1 Net: NC2.NPS.N222S1
W840	Base: LD.HA.FM139s Net: NS.NP.N259*
T64x	Base: LD.ST.FM152s Net: NS.NP.N259*
C935dn	Base: LC.JO.P051S1 Net: NC.NPS.N129S1
C920	Base: LD.TA.FM130s Net: NS.NP.N219S1
C78x	Base: LC.IO.P165aS1 Net: NC2.NPS.N222S1
C77x	Base: LC.CM.P027bS1 Net: NCC.NPS.N107S1
C53x	Base: LS.SW.P026avcS1 Net: NSF.NP.N026S1
C52x	Base: LD.FA.FM131s Net: NS.NP.N219S1

*A network firmware update is required AFTER the base has been updated for this device.

Barcode DLE Versions and Fixes

Updated software that removes the vulnerability described in this advisory is available for the following devices:

Lexmark Models	**Fixed Releases**
X94x	Base: LC.BR.P051HDs1 Net: NC.NPS.N129S1
X85x	Base: LC4.BE.P457S1 Net: NC2.NPS.N222S1
X782e	Base: LC2.TO.P305cS1 Net: NC2.NPS.N222S1
X772e	Base: LC2.TR.P275S1 Net: NC2.NPS.N222S1
X644 & X646	Base: LC2.MC.P307aS1 Net: NC2.NPS.N222S1
X64xef	Base: LC2.TI.P305aS1 Net: NC2.NPS.N222S1
X642	Base: LC2.MB.P307bS1 Net: NC2.NPS.N222S1
W840	Base: LD.HA.BC104s Net: NS.NP.N259*
T64x	Base: LS.ST.P240S1 Net: NS.NP.N219S1
C935dn	Base: LC.JO.P051S1 Net: NC.NPS.N129S1
C920	Base: LD.TA.BC109s Net: NS.NP.N219S1
C78x	Base: LC.IO.P165aS1 Net: NC2.NPS.N222S1
C77x	Base: LC.CM.P027bS1 Net: NCC.NPS.N107S1
C53x	Base: LS.SW.P026avcS1 Net: NSF.NP.N026S1
C52x	Base: LS.FA.P129S1 Net: NS.NP.N219S1

*A network firmware update is required AFTER the base has been updated for this device.

Prescribe DLE Versions and Fixes

Updated software that removes the vulnerability described in this advisory is available for the following devices:

Lexmark Models	**Fixed Releases**
X94x	Base: LC.BR.P051HDs1 Net: NC.NPS.N129S1
X85x	Base: LC4.BE.P457S1 Net: NC2.NPS.N222S1
X782e	Base: LC2.TO.P305cS1

	Net: NC2.NPS.N222S1
X644 & X646	Base: LC2.MC.P307aS1 Net: NC2.NPS.N222S1
X64xef	Base: LC2.TI.P305aS1 Net: NC2.NPS.N222S1
X642	Base: LC2.MB.P307bS1 Net: NC2.NPS.N222S1
W840	Base: LS.HA.P121S1 Net: NS.NP.N118S1
T64x	Base: LS.ST.P240S1 Net: NS.NP.N219S1
C935dn	Base: LC.JO.P051S1 Net: NC.NPS.N129S1
C78x	Base: LC.IO.P165aS1 Net: NC2.NPS.N222S1
C77x	Base: LC.CM.P027bS1 Net: NCC.NPS.N107S1

PrintCryption DLE Versions and Fixes

Updated software that removes the vulnerability described in this advisory is available for the following devices:

Lexmark Models	**Fixed Releases**
X94x	Base: LC.BR.P051HDs1 Net: NC.NPS.N129S1
X85x	Base: LC4.BE.P457S1 Net: NC2.NPS.N222S1
X644 & X646	Base: LC2.MC.P307aS1 Net: NC2.NPS.N222S1
X642	Base: LC2.MB.P307bS1 Net: NC2.NPS.N222S1
W840	Base: LS.HA.P236LPCs Net: NS.NP.N234LPCs
T64x	Base: LS.ST.P240LPCs Net: NS.NP.N234LPCs
C935dn	Base: LC.JO.P051S1 Net: NC.NPS.N129S1
C920	Base: LS.TA.P127LPCs Net: NS.NP.N234LPCs
C78x	Base: LC.IO.P165aS1 Net: NC2.NPS.N222S1
C77x	Base: LC.CM.P027bLPCs Net: NCC.NPS.N116LPs
C53x	Base: LS.SW.P027LPCs Net: NSF.NP.N019LPCs
C52x	Base: LS.FA.P129LPCs Net: NS.NP.N234LPCs

Workarounds

Disabling the embedded web server support for SSL/TLS on the printer (TCP ports 443) blocks the ability to exploit this vulnerability.

If the embedded web server's support for SSL/TLS must remain enabled, the problem can be mitigated by restricting the network devices that are permitted to communicate with the printer. This can be accomplished by utilizing either the "Restricted Server List" feature, or via IPsec configuration on the printers that support these features. Restricting the number of devices that can communicate with the printer limits the devices that can attempt to exploit the vulnerability.

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.

Exploitation and Public Announcements

Lexmark is not aware of any malicious use of the vulnerability described in this advisory

More information on the vulnerability is available at http://www.openssl.org/news/secadv_20040317.txt

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	26 Apr 2010	Initial public announcement
1.1	19-July-2021	Updated legal notice.