Lexmark Security Advisory:

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

Summary

HTTP Denial of service vulnerability.

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

References

CVE: CVE-2010-0101

Affected Products

Selected Lexmark Laser & Inkjet printer products and MarkNet devices; for specific details see "Software Versions & Fixes" below.

Details

Invalid characters in the HTTP header "Authorization" field will cause the embedded HTTP server to crash which halts the operating system. This affects all TCP services on the printer (ports 80, 443, 8000 & 631) that use the HTTP protocol.

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 7.8

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

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.P049 and previous	Base: LC.BR.P051HDs

	Net: NC.NPS.N129 and previous	Net: NC.NPS.N129S
X86x	Base: LP.SP.P112 and previous Net: NR.APS.N332 and previous	Base: LP.SP.P311e and later Net: NP.APS.N332a and later
X85x	Base: LC4.BE.P457 and previous Net: NC2.NPS.N222 and previous	Base: LC4.BE.P457S Net: NC2.NPS.N222S
X782e	Base: LC2.TO.P305c and previous Net: NC2.NPS.N222 and previous	Base: LC2.TO.P305cS Net: NC2.NPS.N222S
X772e	Base: LC.TR.P275 and previous Net: NC2.NPS.N222 and previous	Base: LC2.TR.P275S Net: NC2.NPS.N222S
X73x	Base: LR.FL.P224b and previous Net: NR.APS.N447a and previous	Base: LR.FL.P311e and later Net: NR.APS.N447b and later
X65x	Base: LR.MN.P224a and previous Net: NR.APS.N447a and previous	Base: LR.MN.P311e and later Net: NR.APS.N447b and later
X644 & X646	Base: LC2.MC.P307a and previous Net: NC2.NPS.N222S and previous	Base: LC2.MC.P307aS Net: NC2.NPS.N222S
X64xef	Base: LC2.TI.P305a and previous Net: NC2.NPS.N222 and previous	Base: LC2.TI.P305aS Net: NC2.NPS.N222S
X642	Base LC2.MB.P307b and previous Net: NC2.NPS.N222 and previous	Base: LC2.MB.P307bS Net: NC2.NPS.N222S
X546	Base: LL.EL.P424 and previous Net: NR.APS.N448 and previous	Base: LL.EL.P429a and later Net: NR.APS.N449 and later
X543 & X544	Base: LL.EL.P424 and previous Net: NR.APS.N448 and previous	Base: LL.EL.P429a and later Net: NR.APS.N449 and later
X46x	Base: LR.BS.P224a and previous Net: NR.APS.N447a and previous	Base: LR.BS.P311e and later Net: NR.APS.N447b and later
X36x & X26x	Base: LL.BZ.P424 and previous Net: NR.APS.N448 and previous	Base: LL.BZ.P429a and later Net: NR.APS.N449 and later
X20x	Base: LM1.MT.P110h and previous Net: NM.APS.N048 and previous	Base: LM1.MT.P214 and later Net: NM.APS.N049 and later
W840	Base: LS.HA.P121 and previous Net: NS.NP.N118 and previous	Base: LS.HA.P121S Net: NS.NP.N118S
W850	Base: LP.JB.P108WS and previous Net: NR.APS.N332 and previous	Base: LP.JB.P311e and later Net: NP.APS.N332a and later
T656	Base: LSJ.SJ.P019 and previous Net: NR.APS.N402 and previous	Base: LSJ.SJ.P019S1 and later Net: NR.APS.N402S and later
T650 T652 T654	Base: LR.JP.P224a and previous Net: NR.APS.N447a and previous	Base: LR.JP.P311e and later Net: NR.APS.N447b and later
T64x	Base: LS.ST.P240 and previous Net: NS.NP.N219 and previous	Base: LS.ST.P240S Net: NS.NP.N219S
N4000	Net: PH2.ME.N134 and previous	Net: LC.MD.P012d
N4050e	Net: GO.GO.N106 and previous	Net: GO.GO.N206
N70xxe	Net: LC.CO.N054 and previous	Net: LC.CO.N069
N8120 N8130	Net: NR.APS.N368 and previous	Net: NR.APS.447c
E462	LR.LBH.P224cWS and previous Net: NR.APS.N447a and previous	Base: LR.LBH.P311e and later Net: NR.APS.N447b and later
E460	LR.LBH.P224a and previous Net: NR.APS.N447a and previous	Base: LR.LBH.P311e and later Net: NR.APS.N447b and later
E450	Base: LM.SZ.P113vcREF and previous Net: NM.NA.N098a and previous	Base: LM.SZ.P113vcREs Net: NM.NA.N098aS
E360dn	Base: LL.LBM.P424 and previous Net: NR.APS.N448 and previous	Base: LL.LBM.P429a and later Net: NR.APS.N449 and later

E260 E360d	Base: LL.LBL.P424 and previous Net: NR.APS.N448 and previous	Base: LL.LBL.P429a and later Net: NR.APS.N449 and later
C935dn	LC.JO.P051 and previous Net: NC.NPS.N129 and previous	Base: LC.JO.P051S Net: NC.NPS.N129S
C920	Base: LS.TA.P127 and previous Net: NS.NP.N219 and previous	Base: LS.TA.P127S Net: NS.NP.N219S
C78x	Base: LC.IO.P165a and previous Net: NC2.NPS.N222 and previous	Base: LC.IO.P165aS Net: NC2.NPS.N222S
C77x	Base: LC.CM.P027b and previous Net: NCC.NPS.N107 and previous	Base: LC.CM.P027bS Net: NCC.NPS.N107S
C73x	Base: LR.SK.P224a and previous Net: NR.APS.N447a and previous	Base: LR.SK.P311e and later Net: NR.APS.N447b and later
C546	Base: LU.AS.P424 and previous Net: NR.APS.N448 and previous	Base: LU.AS.P429a and later Net: NR.APS.N449 and later
C540 C543 C544	Base: LL.AS.P424 and previous Net: NR.APS.N448 and previous	Base: LL.AS.P429a and later Net: NR.APS.N449 and later
C53x	Base: LS.SW.P026avc and previous Net: NSF.NP.N026 and previous	Base: LS.SW.P026avcS Net: NSF.NP.N026S
C52x	Base: LS.FA.P129 and previous Net: Net: NS.NP.N219 and previous	Base: LS.FA.P129S Net: NS.NP.N219S
25xxN	Base: LCL.CU.P105 and previous Net: NCL.NA.N104 and previous	Base: LC.CU.P106 and later Net: NCL.NA.N105 and later
X422	GN.AQ.P202 and previous	No release planned, see workaround.
X34x	401.ec4 and previous	No release planned, see workaround.
T430	JX.JU.P101 and previous	No release planned, see workaround.
E350	LE.PH.P121 and previous	No release planned, see workaround.
E34x	BR.H.P204 and previous	No release planned, see workaround.
E33x E23x	141.C09 and previous	No release planned, see workaround.
E250	LE.PM.P121 and previous	No release planned, see workaround.
E240n	BR.Q.P204 and previous	No release planned, see workaround.
E240 E238	BR.M.P204 and previous	No release planned, see workaround.
E120	LE.UL.P040 and previous	No release planned, see workaround.
C510	891.004 and previous	No release planned, see workaround.

IPDS DLE Versions and Fixes

Lexmark Models	**Fixed Releases**
X94x	Base: LC.BR.P051HDs1 Net: NC.NPS.N129S1
X86x	Base: LP.SP.P311h and later Net: NP.APS.332a and later
X85x	Base: LC4.BE.P457S1 Net: NC2.NPS.N222S1
X782e	Base: LC2.TO.P305cS1 Net: NC2.NPS.N222S1
X73x	Base: LR.FL.P311h and later Net: NR.APS.N447b and later
X65x	Base: LR.MN.P311h and later Net: NR.APS.N447b and later

X644 & X646	Base: LC2.MC.P307aS1 Net: NC2.NPS.N222S1
X64xef	Base: LC2.TI.P305aS1 Net: NC2.NPS.N222S1
X46x	Base: LR.BS.P311h and later Net: NR.APS.N447b and later
W840	Base: LS.HA.P225S Net: NS.NP.N259*
W850	Base: LP.JB.P311h and later Net: NP.APS.332a and later
T656	Base: LSJ.SJ.P019S1 and later Net: NR.APS.N402S and later
T650 T652 T654	Base: LR.JP.P311h and later Net: NR.APS.N447b and later
T64x	Base: LS.ST.P240S1 Net: NS.NP.N219S1
E462	Base: LR.LBH.P311h and later Net: NR.APS.N447b and later
E460	Base: LR.LBH.P311h and later Net: NR.APS.N447b and later
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
C73x	Base: LR.SK.P311h and later Net: NR.APS.N447b and later

*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
X86x	Base: LP.SP.P311e and later Net: NP.APS.332a and later
X85x	Base: LC4.BE.P457S1 Net: NC2.NPS.N222S1
X782e	Base: LC2.TO.P305cS1 Net: NC2.NPS.N222S1
X73x	Base: LR.FL.P311e and later Net: NR.APS.N447b and later
X65x	Base: LR.MN.P311e and later Net: NR.APS.N447b and later
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
X46x	Base: LR.BS.P311e and later Net: NR.APS.N447b and later
W840	Base: LD.HA.FM139s Net: NS.NP.N259*
W850	Base: LP.JB.P311e and later Net: NP.APS.332a and later
T656	Base: LSJ.SJ.P019S1 and later Net: NR.APS.N402S and later
T650 T652 T654	Base: LR.JP.P311e and later Net: NR.APS.N447b and later
T64x	Base: LD.ST.FM152s Net: NS.NP.N259*
E462	Base: LR.LBH.P311e and later Net: NR.APS.N447b and later
E460	Base: LR.LBH.P311e and later Net: NR.APS.N447b and later
E450	Base: LM.SZ.P113vcREs Net: NM.NA.N098aS
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
C73x	Base: LR.SK.P311e and later Net: NR.APS.N447b and later
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
X86x	Base: LP.SP.P311e and later Net: NP.APS.332a and later

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
X73x	Base: LR.FL.P311e and later Net: NR.APS.N447b and later
X65x	Base: LR.MN.P311e and later Net: NR.APS.N447b and later
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
X46x	Base: LR.BS.P311e and later Net: NR.APS.N447b and later
W840	Base: LD.HA.BC104s Net: NS.NP.N259*
W850	Base: LP.JB.P311e and later Net: NP.APS.332a and later
T656	Base: LSJ.SJ.P019S1 and later Net: NR.APS.N402S and later
T650 T652 T654	Base: LR.JP.P311e and later Net: NR.APS.N447b and later
T64x	Base: LS.ST.P240S1 Net: NS.NP.N219S1
E462	Base: LR.LBH.P311e and later Net: NR.APS.N447b and later
E460	Base: LR.LBH.P311e and later Net: NR.APS.N447b and later
E450	Base: LM.SZ.P113vcREs Net: NM.NA.N098aS
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
C73x	Base: LR.SK.P311e and later Net: NR.APS.N447b and later
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
X86x	Base: LP.SP.P311e and later Net: NP.APS.332a and later
X85x	Base: LC4.BE.P457S1 Net: NC2.NPS.N222S1
X782e	Base: LC2.TO.P305cS1 Net: NC2.NPS.N222S1
X73x	Base: LR.FL.P311e and later Net: NR.APS.N447b and later
X65x	Base: LR.MN.P311e and later Net: NR.APS.N447b and later
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
X46x	Base: LR.BS.P311e and later Net: NR.APS.N447b and later
W840	Base: LS.HA.P121S1 Net: NS.NP.N118S1
W850	Base: LP.JB.P311e and later Net: NP.APS.332a and later
T656	Base: LSJ.SJ.P019S1 and later Net: NR.APS.N402S and later
T650 T652 T654	Base: LR.JP.P311e and later Net: NR.APS.N447b and later
T64x	Base: LS.ST.P240S1 Net: NS.NP.N219S1
E462	Base: LR.LBH.P311e and later Net: NR.APS.N447b and later
E460	Base: LR.LBH.P311e and later Net: NR.APS.N447b and later
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
C73x	Base: LR.SK.P311e and later Net: NR.APS.N447b and later

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
X86x	Base: LP.SP.P311e and later Net: NP.APS.332a and later
X85x	Base: LC4.BE.P457S1 Net: NC2.NPS.N222S1
X73x	Base: LR.FL.P311e and later Net: NR.APS.N447b and later
X65x	Base: LR.MN.P311e and later Net: NR.APS.N447b and later
X644 & X646	Base: LC2.MC.P307aS1 Net: NC2.NPS.N222S1
X642	Base: LC2.MB.P307bS1 Net: NC2.NPS.N222S1
X46x	Base: LR.BS.P311e and later Net: NR.APS.N447b and later
W840	Base: LS.HA.P236LPCs Net: NS.NP.N234LPCs
W850	Base: LP.JB.P311e and later Net: NP.APS.332a and later
T656	Base: LSJ.SJ.P019S1 and later Net: NR.APS.N402S and later
T650 T652 T654	Base: LR.JP.P311e and later Net: NR.APS.N447b and later
T64x	Base: LS.ST.P240LPCs Net: NS.NP.N234LPCs
E462	Base: LR.LBH.P311e and later Net: NR.APS.N447b and later
E460	Base: LR.LBH.P311e and later Net: NR.APS.N447b and later
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
C73x	Base: LR.SK.P311e and later Net: NR.APS.N447b and later
C53x	Base: LS.SW.P027LPCs Net: NSF.NP.N019LPCs
C52x	Base: LS.FA.P129LPCs Net: NS.NP.N234LPCs

Workarounds

Disabling the HTTP based service on the printer (TCP ports 80, 443, 8000 & 631) blocks the ability to exploit this vulnerability.

If any of the HTTP based services 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

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