Lexmark Security Advisory:

Revision: 1.1
Last update: 19 July 2021
Public Release Date: 22 Mar 2010

Summary

FTP Denial of service vulnerability

Some Lexmark Printers and MarkNet devices contain denial of service vulnerabilities in the FTP service. These vulnerabilities can be exploited with repeated aborted FTP connections to the printer, causing the printer to ignore incoming TCP network connections to multiple services.

References

CVE: CVE-2010-0618

Affected Products

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

Details

Lexmark products have connection flood protection mechanisms that limit the number of simultaneous network connections that can be made to the device on most TCP service ports. (21/FTP 79/Finger, 515/LPD, 631/IPP, 5001, 9100-9104, 9200, 9300, 9400, 9500-9501 & 9600) The FTP service exception handler does not properly maintain the state of the flood protection when passive FTP connections are aborted. Once a sufficient number of passive FTP connections have timed out (typically 15), the flood protection is enabled and is never reset.

The flood protection can be reset by resetting the network adapter, or by power cycling the device.

The firmware update that resolves this vulnerability automatically resets the flood protection after the "Network Job Timeout" has expired or 90 seconds if the "Network Job Timeout" is disabled.

Impact

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

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
Z2420	NET.AR.N204 and previous	NET.AR.N205 and later
Z15xx	NET.MH.N206 and previous	NET.MH.N207 and later
Z1420	NET.MH.N206 and previous	NET.MH.N207 and later
X9575	NET.CH.N208 and previous	NET.CH.N209 and later
X9350	LC.DA.P076 and previous	LC.DA.P077 and later
X7675	NET.CH.N208 and previous	NET.CH.N209 and later
X7550	NET.MH.N206 and previous	NET.MH.N207 and later
X6650	NET.AR.N204 and previous	NET.AR.N205 and later
X6570	NET.MH.N206 and previous	NET.MH.N207 and later
X4975	NET.AR.N204 and previous	NET.AR.N205 and later
X4875	NET.MH.N206 and previous	NET.MH.N207 and later
X4650	NET.AR.N204 and previous	NET.AR.N205 and later
X4550	NET.MH.N206 and previous	NET.MH.N207 and later
X4975VE	NET.CH.N208 and previous	NET.CH.N209 and later
X94x	LC.BR.P049 and previous	LC.BR.P051HDs and later
X86x	LP.SP.P112 and previous	LP.LP.P311e and later
X85x	LC4.BE.P457 and previous	LC4.BE.P457S and later
X782e	LC2.TO.P305c and previous	LC2.TO.P305cS and later
X772e	LC.TR.P275 and previous	LC2.TR.P275S and later
X73x	LR.FL.P224b and previous	LR.FL.P311e and later
X65x	LR.MN.P224a and previous	LR.MN.P311e and later
X644 & X646	LC2.MC.P307a and previous	LC2.MC.P307aS and later
X64xef	LC2.TI.P305a and previous	LC2.TI.P305aS and later
X642	LC2.MB.P307b and previous	LC2.MB.P307bS and later
X546	LL.EL.P424 and previous	LL.EL.P429a and later
X543 & X544	LL.EL.P424 and previous	LL.EL.P429a and later
X46x	LR.BS.P224a and previous	LR.BS.P311e and later
X36x & X26x	LL.BZ.P424 and previous	LL.BZ.P429a and later
X20x	LM1.MT.P110h and previous	LM1.MT.P214 and later
W840	LS.HA.P121 and previous	LS.HA.P121S and later
W850	LP.JB.P108WS and previous	LP.JB.P311e and later
T656	LSJ.SJ.P019 and previous	LSJ.SJ.P019S and later
T650 T652 T654	LR.JP.P224a and previous	LR.JP.P311e and later
T64x	LS.ST.P240 and previous	LS.ST.P240S and later
N4000	PH2.ME.N134 and previous	LC.MD.P012d and later
N4050e	GO.GO.N106 and previous	GO.GO.N206 and later
N70xxe	LC.CO.N054 and previous	LC.CO.N069 and later
N8120 N8130	NR.APS.N368 and previous	NR.APS.447c and later
E462	LR.LBH.P224cWS and previous	LR.LBH.P311e and later
E460	LR.LBH.P224a and previous	LR.LBH.P311e and later
E450	LM.SZ.P113vcREF and previous	LM.SZ.P113vcREs and later
E360dn	LL.LBM.P424 and previous	LL.LBM.P429a and later
E260 E360d	LL.LBL.P424 and previous	LL.LBL.P429a and later
C935dn	LC.JO.P051 and previous	LC.JO.P051S and later

C920	LS.TA.P127 and previous	LS.TA.P127S and later
C78x	LC.IO.P165a and previous	LC.IO.P165aS and later
C77x	LC.CM.P027b and previous	LC.CM.P027bS and later
C73x	LR.SK.P224a and previous	LR.SK.P311e and later
C546	LU.AS.P424 and previous	LU.AS.P429a and later
C540 C543 C544	LL.AS.P424 and previous	LL.AS.P429a and later
C53x	LS.SW.P026avc and previous	LS.SW.P026avcS and later
C52x	LS.FA.P129 and previous	LS.FA.P129S and later
25xxN	LCL.CU.P105 and previous	LC.CU.P106 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	LC.BR.P051HDs1 and later
X86x	LP.LP.P311h and later
X85x	LC4.BE.P457S1 and later
X782e	LC2.TO.P305cS1 and later
X73x	LR.FL.P311h and later
X65x	LR.MN.P311h and later
X644 & X646	LC2.MC.P307aS1 and later
X64xef	LC2.TI.P305aS1 and later
X46x	LR.BS.P311h and later
W840	LS.HA.P225S and later
W850	LP.JB.P311h and later
T656	LSJ.SJ.P019S and later
T650 T652 T654	LR.JP.P311h and later
T64x	LS.ST.P240S1 and later
E462	LR.LBH.P311h and later
E460	LR.LBH.P311h and later
C935dn	LC.JO.P051S1 and later
C920	LS.TA.P127EPs and later
C78x	LC.IO.P165aS1 and later
C77x	LC.CM.P027bS1 and later
C73x	LR.SK.P311h and later

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	LC.BR.P051HDs1 and later
X86x	LP.LP.P311e and later
X85x	LC4.BE.P457S1 and later
X782e	LC2.TO.P305cS1 and later
X73x	LR.FL.P311e and later
X65x	LR.MN.P311e and later
X644 & X646	LC2.MC.P307aS1 and later
X64xef	LC2.TI.P305aS1 and later
X642	LC2.MB.P307bS1 and later
X46x	LR.BS.P311e and later
W840	LD.HA.FM139s and later
W850	LP.JB.P311e and later
T656	LSJ.SJ.P019S and later
T650 T652 T654	LR.JP.P311e and later
T64x	LD.ST.FM152s and later
E462	LR.LBH.P311e and later
E460	LR.LBH.P311e and later
E450	LM.SZ.P113vcREs1 and later
C935dn	LC.JO.P051S1 and later
C920	LD.TA.FM130s and later
C78x	LC.IO.P165aS1 and later
C77x	LC.CM.P027bS1 and later
C73x	LR.SK.P311e and later
C53x	LS.SW.P026avcS1 and later
C52x	LD.FA.FM131s and later

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	LC.BR.P051HDs1 and later
X86x	LP.LP.P311e and later
X85x	LC4.BE.P457S1 and later
X782e	LC2.TO.P305cS1 and later
X772e	LC2.TR.P275S1 and later
X73x	LR.FL.P311e and later
X65x	LR.MN.P311e and later
X644 & X646	LC2.MC.P307aS1 and later
X64xef	LC2.TI.P305aS1 and later
X642	LC2.MB.P307bS1 and later

X46x	LR.BS.P311e and later
W840	LD.HA.BC104s and later
W850	LP.JB.P311e and later
T656	LSJ.SJ.P019S and later
T650 T652 T654	LR.JP.P311e and later
T64x	LS.ST.P240S1 and later
E462	LR.LBH.P311e and later
E460	LR.LBH.P311e and later
E450	LM.SZ.P113vcREs1 and later
C935dn	LC.JO.P051S1 and later
C920	LD.TA.BC109s and later
C78x	LC.IO.P165aS1 and later
C77x	LC.CM.P027bS1 and later
C73x	LR.SK.P311e and later
C53x	LS.SW.P026avcS1 and later
C52x	LS.FA.P129S1 and later

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	LC.BR.P051HDs1 and later
X86x	LP.LP.P311e and later
X85x	LC4.BE.P457S1 and later
X782e	LC2.TO.P305cS1 and later
X73x	LR.FL.P311e and later
X65x	LR.MN.P311e and later
X644 & X646	LC2.MC.P307aS1 and later
X64xef	LC2.TI.P305aS1 and later
X642	LC2.MB.P307bS1 and later
X46x	LR.BS.P311e and later
W840	LS.HA.P121S1 and later
W850	LP.JB.P311e and later
T656	LSJ.SJ.P019S and later
T650 T652 T654	LR.JP.P311e and later
T64x	LS.ST.P240S1 and later
E462	LR.LBH.P311e and later
E460	LR.LBH.P311e and later
C935dn	LC.JO.P051S1 and later
C78x	LC.IO.P165aS1 and later
C77x	LC.CM.P027bS1 and later
C73x	LR.SK.P311e 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	LC.BR.P051HDs1 and later
X86x	LP.LP.P311e and later
X85x	LC4.BE.P457S1 and later
X73x	LR.FL.P311e and later
X65x	LR.MN.P311e and later
X644 & X646	LC2.MC.P307aS1 and later
X642	LC2.MB.P307bS1 and later
X46x	LR.BS.P311e and later
W840	LS.HA.P236LPCs and later
W850	LP.JB.P311e and later
T656	LSJ.SJ.P019S and later
T650 T652 T654	LR.JP.P311e and later
T64x	LS.ST.P240LPCs and later
E462	LR.LBH.P311e and later
E460	LR.LBH.P311e and later
C935dn	LC.JO.P051S1 and later
C920	LS.TA.P127LPCs and later
C78x	LC.IO.P165aS1 and later
C77x	LC.CM.P027bLPCs and later
C73x	LR.SK.P311e and later
C53x	LS.SW.P027LPCs and later
C52x	LS.FA.P129LPCs and later

Workarounds

Disabling the FTP service on the printer blocks the ability to exploit this vulnerability.

If the FTP service must be left 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 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

Lexmark would like to thank Francis Provencher of Protek Research Labs for bringing this to our attention.

Status of this Notice:

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	22-Mar-2010	Initial Public Release
1.1	19-July-2021	Updated legal notice.