Lexmark Security Advisory:

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

Summary

PJL Remote buffer overflow vulnerability.

Some Lexmark Laser Printers contain remote buffer overflow vulnerabilities in their PJL processing functionality. These vulnerabilities could potentially lead to remote code execution, but no malicious use of this vulnerability is known.

References

CVE: CVE-2010-0619

Affected Products

Multiple Lexmark laser printer products, for specific details see "Software Versions & Fixes" below.

Details

If a specifically crafted PJL command is sent to the printer, it is possible to insert information onto the stack of the embedded microprocessor.

Impact

Successful exploitation of this vulnerability can lead to remote code execution on the affected printer.

Vulnerability Scoring Details

CVSS Base Score 7.3

Exploitability:		Impact:	
Access Vector:	Network	Confidentiality:	Complete
Access Complexity:	High	Integrity:	Partial
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	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	LC2.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	LL.BZ.P424 and previous	LL.BZ.P429a and later
X264	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
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

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

The problem can be mitigated by restricting the network devices that are permitted to communicate with the printer.

This can be accomplished by:

- Limiting access to the printer by utilizing either the "**Restricted Server List**" feature, or **IPsec** if the printer supports this feature. By restricting the number of devices that can communicate with the printer, you limit the number of devices that can be exploited by the vulnerability.
- Power cycling the printer will remove any injected code, and remove any resulting 900 service error.
- Enable automatic HDD wiping on the device to eliminate risk associated to residual job data.

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:

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