Lexmark Security Advisory:

Revision: 1.1
Last update: 23 July 2021
Public Release Date: 19 February 2015

Summary

GHOST: glibc gethostbyname buffer overflow vulnerability

A vulnerability was disclosed in the “glibc” library that provides the potential for an attacker to execute arbitrary code on an affected system.

References

CVE: CVE-2015-0235

Details

On January 27 2015 a buffer overflow vulnerability was announced in the glibc library function __nss_hostname_digits_dots().This vulnerability can be leveraged to execute arbitrary code.

Lexmark printer products contain the vulnerability, but are not susceptable to any of the known exploit methods; therefore abusing the vulnerability on a Lexmark device is difficult.

CVSS	Base Score	7.6	(AV:L/AC:H/AU:N/C:N/I:P/A:C)
	Impact Subscore:	10	
	Exploitability Subscore:	4.9	

CVSS scores are calculated in accordance with CVSS version 2.0 (http://www.first.org/cvss/cvss-guide.html)

Impact

Successful exploitation of this vulnerability can lead to the disclosure and/or modification of information and the ability to execute code on the affected system.

Affected Products

The following products are known to be affected, for specific details see “Product Specific Information” below. Lexmark is assessing each product and will update this advisory as more information becomes available.

- Lexmark printer products

Product Specific Information

Lexmark is individually assessing each product and will update this advisory as more information becomes available.

Laser printer products

The following printers and MFPs are affected:

To determine a devices firmware level, select the "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 upgrade to a "Fixed Release".

Lexmark Models	**Affected Releases**	**Fixed Releases**
CS31x	LW41.VYL.P481 and previous	LW41.VYL.P482 and later
CS41x	LW41.VY2.P481 and previous	LW41.VY2.P482 and later
CS51x	LW41.VY4.P481 and previous	LW41.VY4.P482 and later
CX310	LW41.GM2.P481 and previous	LW41.GM2.P482 and later
CX410	LW41.GM4.P481 and previous	LW41.GM4.P482 and later
CX510	LW41.GM7.P481 and previous	LW41.GM7.P482 and later
XC2132	LW41.GM7.P481 and previous	LW41.GM7.P482 and later
MS310	LW41.PRL.P481 and previous	LW41.PRL.P482 and later
MS312	LW41.PRL.P481 and previous	LW41.PRL.P482 and later
MS315	LW41.TL.P481 and previous	LW41.TL.P482 and later
MS410	LW41.PRL.P481 and previous	LW41.PRL.P482 and later
MS415	LW41.TL.P481 and previous	LW41.TL.P482 and later
MS51x	LW41.PR2.P481 and previous	LW41.PR2.P482 and later
MS610dn & MS610dtn	LW41.PR2.P481 and previous	LW41.PR2.P482 and later
M1145 & M3150dn	LW41.PR2.P481 and previous	LW41.PR2.P482 and later
MS610de & MS610dte	LW41.PR4.P481 and previous	LW41.PR4.P482 and later
M3150	LW41.PR4.P481 and previous	LW41.PR4.P482 and later
MS71x	LW41.DN2.P481 and previous	LW41.DN2.P482 and later
MS810n, MS810dn & MS810dtn	LW41.DN2.P481 and previous	LW41.DN2.P482 and later
MS811	LW41.DN2.P481 and previous	LW41.DN2.P482 and later
MS812dn, MS812dtn	LW41.DN2.P481 and previous	LW41.DN2.P482 and later
M5163dn	LW41.DN2.P481 and previous	LW41.DN2.P482 and later
MS810de	LW41.DN4.P481 and previous	LW41.DN4.P482 and later
M5155 & M5163	LW41.DN4.P481 and previous	LW41.DN4.P482 and later
MS812de	LW41.DN7.P481 and previous	LW41.DN7.P482 and later
M5170	LW41.DN7.P481 and previous	LW41.DN7.P482 and later
MS91x	LW41.SA.P481 and previous	LW41.SA.P482 and later
MX310	LW41.SB2.P481 and previous	LW41.SB2.P482 and later
MX410, MX510 & MX511	LW41.SB4.P481 and previous	LW41.SB4.P482 and later
XM1145	LW41.SB4.P481 and previous	LW41.SB4.P482 and later
MX610 & MX611	LW41.SB7.P481 and previous	LW41.SB7.P482 and later
XM3150	LW41.SB7.P481 and previous	LW41.SB7.P482 and later
MX71x	LW41.TU.P481 and previous	LW41.TU.P482 and later
MX81x	LW41.TU.P481 and previous	LW41.TU.P482 and later
XM51xx & XM71xx	LW41.TU.P481 and previous	LW41.TU.P482 and later
MX91x	LW41.MG.P481 and previous	LW41.MG.482 and later
MX6500e	LW41.JD.P482 and previous	LW41.JD.483 and later
C746	LHS41.CM2.P471 and previous	LHS41.CM2.P472 and later
C748 & CS748	LHS41.CM4.P471 and previous	LHS41.CM4.P472 and later
C79x & CS796	LHS41.HC.P471 and previous	LHS41.HC.P472 and later
C925	LHS41.HV.P471 and previous	LHS41.HV.P472 and later
C95x	LHS41.TP.P471 and previous	LHS41.TP.P472 and later

X548 & XS548	LHS41.VK.P471 and previous	LHS41.VK.P472 and later
X74x & XS748	LHS41.NY.P471 and previous	LHS41.NY.P472 and later
X792 & XS79x	LHS41.MR.P471 and previous	LHS41.MR.P472 and later
X925 & XS925	LHS41.HK.P471 and previous	LHS41.HK.P472 and later
X95x & XS95x	LHS41.TQ.P471 and previous	LHS41.TQ.P472 and later
6500e	LHS41.JR.P471 and previous	LHS41.JR.P472 and later
C734	LR.SK.P695 and previous	LR.SK.P696 and later
C736	LR.SKE.P693 and previous	LR.SKE.P694 and later
E46x	LR.LBH.P674 and previous	LR.LBH.P675 and later
T650 & T652	LR.JP.P683 and previous	LR.JP.P684 and later
T654	LR.JP.P683 and previous	LR.JP.P684 and later
T656	LSJ.SJ.P043 and previous	LSJ.SJ.P044 and later
W85x	LR.JB.P646 and previous	LR.JB.P647 and later
X46x	LR.BS.P697 and previous	LR.BS.P698 and later
X65x	LR.MN.P698 and previous	LR.MN.P699 and later
X73x	LR.FL.P697 and previous	LR.FL.P698 and later
X86x	LP.SP.P698 and previous	LP.SP.P699 and later
C54x	In Evaluation	Contact Lexmark
E26x	In Evaluation	Contact Lexmark
E36x	In Evaluation	Contact Lexmark
X26x	In Evaluation	Contact Lexmark
X36x	In Evaluation	Contact Lexmark
X54x	In Evaluation	Contact Lexmark
C52x	In Evaluation	Contact Lexmark
C53x	In Evaluation	Contact Lexmark
C77x	In Evaluation	Contact Lexmark
C78x	In Evaluation	Contact Lexmark
C92x	In Evaluation	Contact Lexmark
C93x	In Evaluation	Contact Lexmark
E45x	In Evaluation	Contact Lexmark
T64x	In Evaluation	Contact Lexmark
W84x	In Evaluation	Contact Lexmark
X642	In Evaluation	Contact Lexmark
X644/X646	In Evaluation	Contact Lexmark
X64xef	In Evaluation	Contact Lexmark
X85x	In Evaluation	Contact Lexmark
X94x	In Evaluation	Contact Lexmark
N4000	LC.MD.P119 and previous	Contact Lexmark
N4050e	GO.GO.N206 and previous	Contact Lexmark
N7xxe	LC.CO.N309 and previous	Contact Lexmark

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. 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	16-Feburary-2015	Initial Public Release
1.1	23-July-2021	Updated legal notice