Lexmark Security Advisory:

Revision: 1.0
Last update: 7 March 2016
Public Release Date: 11 March 2016

Summary

Glibc getaddrinfo() stack buffer overflow.

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

References

CVE: CVE-2015-7547

Details

On February 16, 2016 a buffer overflow vulnerability in glibc was announced in the send_dg() and send_vc() resolver functions was announced. The vulnerable functions can be accessed via getaddrinfo(). These vulnerabilities allow a remote attacker to either crash or execute arbitrary code on a vulnerable system via a crafted DNS response.

CVSSv3 Base Score 8.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
Impact Subscore: 5.9
Exploitability Subscore: 2.2

CVSSv2 Base Score 6.8 (AV:L/AC:M/AU:N/C:P/I:P/A:P)
Impact Subscore: 6.4
Exploitability Subscore: 8.6

CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss/user-guide)
CVSSv2 scores are calculated in accordance with CVSS version 2.0 (https://www.first.org/cvss/v2/guide)

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

To determine a devices firmware level, select the “Settings”->“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
CX820de, CX820dtfe	PP.02.057 and previous	PP.02.058 and later

XC6152de, XC6152dtfe	PP.02.057 and previous	PP.02.058 and later
CX825de, CX825dte, CX825dtfe	PP.02.057 and previous	PP.02.058 and later
XC8155de, XC8155dte	PP.02.057 and previous	PP.02.058 and later
CX860de, CX860dte, CX860dtfe	PP.02.057 and previous	PP.02.058 and later
XC8160de, XC8160dte	PP.02.057 and previous	PP.02.058 and later
CS820de, CS820dte, CS820dtfe	YK.02.057 and previous	YK.02.058 and later
C6160	YK.02.057 and previous	YK.02.058 and later
CS720de, CS720dte	CB.02.057 and previous	CB.02.058 and later
CS725de, CS725dte	CB.02.057 and previous	CB.02.058 and later
C4150	CB.02.057 and previous	CB.02.058 and later
CX725de, CX725dhe, CX725dthe	ATL.02.057 and previous	ATL.02.058 and later
XC4150	ATL.02.057 and previous	ATL.02.058 and later
CS31x	LW50.VYL.P592 and previous, LW60.VYL.P630 & LW60.VYL.P631	LW50.VYL.P593 and later, LW60.VYL.P632 and later
CS41x	LW50.VY2.P592 and previous, LW60.VY2.P630 & LW60.VY2.P631	LW50.VY2.P593 and later, LW60.VY2.P632 and later
CS51x	LW50.VY4.P592 and previous, LW60.VY4.P630 & LW60.VY4.P631	LW50.VY4.P593 and later, LW60.VY4.P632 and later
CX310	LW50.GM2.P592 and previous, LW60.GM2.P630 & LW60.GM2.P631	LW50.GM2.P593 and later, LW60.GM2.P632 and later
CX410	LW50.GM4.P592 and previous, LW60.GM4.P630 & LW60.GM4.P631	LW50.GM4.P593 and later, LW60.GM4.P632 and later
CX510	LW50.GM7.P592 and previous, LW60.GM7.P630 & LW60.GM7.P631	LW50.GM7.P593 and later, LW60.GM7.P632 and later
XC2132	LW50.GM7.P592 and previous, LW60.GM7.P630 & LW60.GM7.P631	LW50.GM7.P593 and later, LW60.GM7.P632 and later
MS310	LW50.PRL.P592 and previous, LW60.PRL.P630 & LW60.PRL.P631	LW50.PRL.P593 and later, LW60.PRL.P632 and later
MS312	LW50.PRL.P592 and previous, LW60.PRL.P630 & LW60.PRL.P631	LW50.PRL.P593 and later, LW60.PRL.P632 and later
MS315	LW50.TL.P592 and previous, LW60.TL.P630 & LW60.TL.P631	LW50.TL.P593 and later, LW60.TL.P632 and later
MS410	LW50.PRL.P592 and previous, LW60.PRL.P630 & LW60.PRL.P631	LW50.PRL.P593 and later, LW60.PRL.P632 and later
MS415	LW50.TL.P592 and previous, LW60.TL.P630 & LW60.TL.P631	LW50.TL.P593 and later, LW60.TL.P632 and later
MS51x	LW50.PR2.P592 and previous, LW60.PR2.P630 & LW60.PR2.P631	LW50.PR2.P593 and later, LW60.PR2.P632 and later

MS610dn & MS610dtn	LW50.PR2.P592 and previous, LW60.PR2.P630 & LW60.PR2.P631	LW50.PR2.P593 and later, LW60.PR2.P632 and later
M1145 & M3150dn	LW50.PR2.P592 and previous, LW60.PR2.P630 & LW60.PR2.P631	LW50.PR2.P593 and later, LW60.PR2.P632 and later
MS610de & MS610dte	LW50.PR4.P592 and previous, LW60.PR4.P630 & LW60.PR4.P631	LW50.PR4.P593 and later, LW60.PR4.P632 and later
M3150	LW50.PR4.P592 and previous, LW60.PR4.P630 & LW60.PR4.P631	LW50.PR4.P593 and later, LW60.PR4.P632 and later
MS71x	LW50.DN2.P592 and previous, LW60.DN2.P630 & LW60.DN2.P631	LW50.DN2.P593 and later, LW60.DN2.P632 and later
MS810n, MS810dn & MS810dtn	LW50.DN2.P592 and previous, LW60.DN2.P630 & LW60.DN2.P631	LW50.DN2.P593 and later, LW60.DN2.P632 and later
MS811	LW50.DN2.P592 and previous, LW60.DN2.P630 & LW60.DN2.P631	LW50.DN2.P593 and later, LW60.DN2.P632 and later
MS812dn, MS812dtn	LW50.DN2.P592 and previous, LW60.DN2.P630 & LW60.DN2.P631	LW50.DN2.P593 and later, LW60.DN2.P632 and later
M5163dn	LW50.DN2.P592 and previous, LW60.DN2.P630 & LW60.DN2.P631	LW50.DN2.P593 and later, LW60.DN2.P632 and later
MS810de	LW50.DN4.P592 and previous, LW60.DN4.P630 & LW60.DN4.P631	LW50.DN4.P593 and later, LW60.DN4.P632 and later
M5155 & M5163	LW50.DN4.P592 and previous, LW60.DN4.P630 & LW60.DN4.P631	LW50.DN4.P593 and later, LW60.DN4.P632 and later
MS812de	LW50.DN7.P592 and previous, LW60.DN7.P630 & LW60.DN7.P631	LW50.DN7.P593 and later, LW60.DN7.P632 and later
M5170	LW50.DN7.P592 and previous, LW60.DN7.P630 & LW60.DN7.P631	LW50.DN7.P593 and later, LW60.DN7.P632 and later
MS91x	LW50.SA.P592 and previous, LW60.SA.P630 & LW60.SA.P631	LW50.SA.P593 and later, LW60.SA.P632 and later
MX310	LW50.SB2.P592 and previous, LW60.SB2.P630 & LW60.SB2.P631	LW50.SB2.P593 and later, LW60.SB2.P632 and later
MX410, MX510 & MX511	LW50.SB4.P592 and previous, LW60.SB4.P630 & LW60.SB4.P631	LW50.SB4.P593 and later, LW60.SB4.P632 and later
XM1145	LW50.SB4.P592 and previous, LW60.SB4.P630 & LW60.SB4.P631	LW50.SB4.P593 and later, LW60.SB4.P632 and later

MX610 & MX611	LW50.SB7.P592 and previous, LW60.SB7.P630 & LW60.SB7.P631	LW50.SB7.P593 and later, LW60.SB7.P632 and later
XM3150	LW50.SB7.P592 and previous, LW60.SB7.P630 & LW60.SB7.P631	LW50.SB7.P593 and later, LW60.SB7.P632 and later
MX71x	LW50.TU.P592 and previous, LW60.TU.P630 & LW60.TU.P631	LW50.TU.P593 and later, LW60.TU.P632 and later
MX81x	LW50.TU.P592 and previous, LW60.TU.P630 & LW60.TU.P631	LW50.TU.P593 and later, LW60.TU.P632 and later
XM51xx & XM71xx	LW50.TU.P592 and previous, LW60.TU.P630 & LW60.TU.P631	LW50.TU.P593 and later, LW60.TU.P632 and later
MX91x	LW50.MG.P592 and previous, LW60.MG.P630 & LW60.MG.P631	LW50.MG.593 and later, LW60.MG.P632 and later
MX6500e	LW50.JD.P592 and previous, LW60.JD.P630 & LW60.JD.P631	LW50.JD.593 and later, LW60.JD.P632 and later

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	7 March 2016	Initial Public Release