Lexmark Security Advisory:

Revision:	1.0
Last update:	10 May 2017
Public Release Date:	25 May 2017

Summary

Some Lexmark products have a remote code execution vulnerability that allows a remote attacker to execute arbitrary code on the device.

References

CVE: CVE-2016-10229

Details

A vulnerability in udp.c in the Linux kernel before 4.5 allows remote attackers to execute arbitrary code via UDP traffic that triggers an unsafe second checksum calculation during execution of a recv system call with the MSG_PEEK flag.

CVSS v3 Base Score:	9.8 Critical	(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Impact Score:	5.9	
Exploitability Score:	3.9	

CVSS v2 Base Score:	10.0 HIGH	(AV:N/AC:L/Au:N/C:C/I:C/A:C)
Impact Subscore:	10.0	
Exploitability Subscore:	10.0	

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

This vulnerability can lead to the unauthorized disclosure of configuration information and user data on the affected device.

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 Releas**e".

Lexmark Models	Affected Releases	Fixed Release
CX820de, CX820dtfe	PP.033.115 and previous	PP. 033.116 and later
XC6152de, XC6152dtfe	PP.033.115 and previous	PP.033.116 and later
CX825de, CX825dte, CX825dtfe	PP.033.115 and previous	PP.033.116 and later
XC8155de, XC8155dte	PP.033.115 and previous	PP.033.116 and later
CX860de, CX860dte, CX860dtfe	PP.033.115 and previous	PP.033.116 and later
XC8160de, XC8160dte	PP.033.115 and previous	PP.033.116 and later
CS820de, CS820dte, CS820dtfe	YK.033.115 and previous	YK.033.116 and later
C6160	YK.033.115 and previous	YK.033.116 and later
CS720de, CS720dte	CB.033.115 and previous	CB.033.116 and later
CS725de, CS725dte	CB.033.115 and previous	CB.033.116 and later
C4150	CB.033.115 and previous	CB.033.116 and later
CX725de, CX725dhe, CX725dthe	ATL.033.115 and previous	ATL.033.116 and later
XC4150	ATL.033.115 and previous	ATL.033.116 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.

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	25 May 2017	Initial Public Release