Lexmark Security Advisory:

Revision: 1.0
Last update: 31 May 2017
Public Release Date: 31 May 2017

Summary

WannaCry Ransomware Vulnerability

Lexmark devices are not vulnerable to WannaCry ransomware or to the following associated exploits: EternalBlue, EternalSynery, EternalRomance, EternalChampion. This attack propagates through Microsoft SMBv1 servers.

References

MS17-010, CVE(s): CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147 and CVE-2017-0148

Details

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB RemoteCode Execution Vulnerability." Lexmark devices do not run Microsoft SMBv1 servers or any other SMB servers, and only run SMB clients through a non-Microsoft implementation.

Impact

These exploits only impact Microsoft SMBv1 servers. Lexmark devices are not vulnerable to WannaCry ransomware or to associated exploits using SMBv1 servers.
This vulnerability can lead to the unauthorized disclosure of configuration information and user data on the affected device.

Affected Products

No Lexmark devices or products are affected by this vulnerability.

Recommendations

Apply the latest security patches to Microsoft Windows systems.

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	31 May 2017	Initial Public Release