Lexmark Security Advisory:

Revision: 1.0
Last update: 18 January 2018
Public Release Date: 18 January 2018

Summary

Some Lexmark devices may contain CPUs that are affected by the speculative execution vulnerabilities known as Spectre (CVE-2017-5753 and CVE-2017-5715) and Meltdown (CVE-2017-5754). However, there is no known path to exploit these vulnerabilities on a Lexmark device.

References

CVE: CVE-2017-5753, CVE-2017-5715, CVE-2017-5754

Details

On January 3, 2018, vulnerabilities were reported in several CPUs that perform speculative execution. The vulnerabilities could at worst be used by an attacker to read arbitrary virtual memory across security boundaries. Several classes of processors have been identified as affected, including those from Intel, AMD, ARM, and IBM.

There are several variants of this speculative execution flaw. The first two, CVE-2017-5753 and CVE-2017-5715, are known as Spectre, and the third, CVE-2017-5754, is known as Meltdown. These are all variants of the same attack and differ in the way the CPU flaw is exploited.

To exploit any of these vulnerabilities, three conditions must be met:

1. The CPU in use must contain the speculative execution vulnerability,
2. The device must allow custom code execution, and
3. A high-resolution timer must be available to distinguish between cache hits and misses

Relevance to Lexmark Devices

Many Lexmark devices utilize speculative execution of instructions to optimize device performance. Several Lexmark devices contain a CPU which may be vulnerable to the Spectre and Meltdown vulnerabilities.

Lexmark devices, however, include protections which mitigate the risk of these vulnerabilities. These include limiting the code that can be executed by the firmware and preventing access to high resolution timers.

The following section provides technical details.

Limits On Custom Code Execution:

To exploit the Spectre vulnerability, one must be able to run custom code on an affected device. Lexmark printers, depending on the model, have the ability to execute the following types of code:

- Lexmark Firmware & Embedded Solutions
- Printer DataStream Languages
- Cloud Solutions

Lexmark Firmware & Embedded Solutions:

Lexmark has designed its firmware and Embedded Solutions such that only code bearing a Lexmark digital signature can be executed. The integrity of the firmware is continuously verified at runtime. This design blocks the execution of arbitrary code, which in turn protects Lexmark devices from threats of this type.

Printer DataStream Languages:

Inherent in the design of some Printer DataStream Languages are instructions that are interpreted. Such interpreted instructions are not converted to native instructions, and are limited by definition in what actions can be performed. One such limitation is that there is no access to high resolution timers needed to exploit the Spectre and Meltdown vulnerabilities.

Cloud Solutions:

Lexmark's Cloud Solutions Framework consists of an embedded web browser that allows Javascript to be executed. Protection features on this platform can prevent the execution of unintended code. The SharedArrayBuffer is not available on any Lexmark device. Analysis shows that the timers available to Javascript are insufficient to distinguish between cache hits and misses, which is necessary to exploit the Spectre and Meltdown vulnerabilities.

Summary:
Lexmark devices are not vulnerable to the Meltdown or Spectre vulnerabilities. While some devices may contain CPUs which are vulnerable to Spectre and Meltdown, security measures used in Lexmark devices mitigate the risk of these vulnerabilities. Because Lexmark devices are not vulnerable to these threats, no firmware updates are planned.

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	18 January 2018	Initial Public Release