Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, California 95403

www.keysight.com

Effective: 02 February 2018

Keysight Technologies, Inc.

Information on “Spectre” and “Meltdown” CPU Vulnerabilities

(INTEL-SA-00088, CVE-2017-5715, CVE-2017-5753 and CVE-2017-5754)

Keysight Technologies is aware of new security research describing vulnerabilities in Intel, AMD and ARM-based CPUs that, when exploited for malicious purposes, could permit collection of data from computing devices that otherwise are operating as designed. These vulnerabilities are commonly known as “speculative execution side-channel attacks” and are also referred to as “Spectre” and “Meltdown”. At this time, Keysight has no information indicating these vulnerabilities have been used to attack our customers.

Keysight is investigating the potential impacts of “Spectre” and “Meltdown” on our products. Several of our modern Microsoft Windows based instruments use Intel processors that contain the vulnerabilities. Most instruments that do not use a “desktop derived” Windows operating system (those using CE, embedded Linux, VxWorks or other embedded operating systems) do not contain processors with the vulnerabilities or are not readily susceptible to exploit. We will publish a list of affected products once our investigation has progressed, and we have recommended mitigation advisement.

Given the apparent instability of the processor software updates supplied by the vendors, Keysight has not yet published BIOS updates, and is recommending customers not attempt a BIOS update until we have had a chance to evaluate the impact of the updates on our products. Windows operating system updates can continue to be installed, as they do not by themselves cause the instabilities. However, it should be noted that the OS updates alone do not mitigate the vulnerabilities. As always, customers should review Microsoft’s information on an update’s compatibility with user installed applications such as anti-malware software.

Check back at the Keysight Product & Solution Cyber Security page for updates.

For reference, information from Microsoft regarding these vulnerabilities can be found at: ADV180002 | Guidance to mitigate speculative execution side-channel vulnerabilities.

Information from Intel can be found at: Security Exploits and Intel Products.