Patton Devices Not Vulnerable to Meltdown and Spectre side-channels attacks

Gaithersburg, January 4, 2018

Patton devices running either Patton's SmartWare or Trinity firmware are not vulnerable to the side-channel attacks commonly known as Meltdown and Spectre.

Meltdown (CVE-2017-5754) and **Spectre** (CVE-2017-5753, CVE-2017-5715) are issues on processors by **Intel**, **AMD**, and **ARM**, where information out of mis-speculated execution is leaked to the CPU data cache and can be exploited by attacker programs [1]. Such programs might gain access to privileged (kernel) memory or to the isolated memory of other processes running on the same vulnerable CPU.

The following Patton devices are powered by ARM CPUs, but those CPU variants are not vulnerable to the issue: **SN53xx**, **CL23xx**, and **OS33xx** devices are equipped with a TI Sitara AM3352 processor, powered by an ARM Cortex-A8 CPU core, variant 3. **SN413x**, **SN414x**, **SN415x**, **SN417x**, and **SN55xx** devices are equipped with a Broadcom BCM5301x processor, powered by an ARM Cortex-A9 CPU core, variant 3. Only variant 1 and 2 of ARM Cortex-A8 and Cortex-A9 cores are potentially affected by the vulnerability, variant 3 of both architectures is not affected [2]. All other Patton devices are equipped with older-generation Freescale CPUs that do not support speculative execution and that are not vulnerable to the Meltdown and Spectre attacks.

Since no CPUs used by Patton Electronics Co. are affected by the issue, Patton devices are not vulnerable to Meltdown or Spectre attacks.

[1] Project Zero: Reading privileged memory with a side channel: https://googleprojectzero.blogspot.ch/2018/01/reading-privileged-memory-with-side.html

[2] ARM: Vulnerability of Speculative Processors to Cache Timing Side-Channel Mechanisms: https://developer.arm.com/support/security-update