Meltdown and Spectre security vulnerabilities

TECHNICAL NOTE

BN-0009-01

AVT
Advanced Virtualization Technologies

vere technologies

MELTDOWN AND SPECTRE SECURITY VULNERABILITIES BN-0009-01 (11-Jan-2018)

vtAlpha and vtVAX are marketed jointly by AVT and Vere Technologies LLC

Table of Contents

1. Impact of Meltdown and Spectre

The impact of the Meltdown and Spectre security vulnerabilities inside the VtServer environment is limited. The reason is that both vulnerabilities are dependent on the ability to run untrusted software on a machine, which is not possible inside the closed VtServer environment (see Section 10.9 of the vtServer Reference Manual for more information).

There is one exception to that which is the embedded web browser (Firefox) that can be run on the console of the system; this opens up the possibility to connect to an outside website which in turn may load malicious java script code. Since this browser is not used in production, and can only be used from the system's console, there will be no harm done as long as it is not used. Notice that the console should be protected from access for normal users in any case.

2. Patch

We can make a patch available on request to remove the possibility to access the browser from the console. In a future update we will introduce an updated Linux kernel that will work around the issue. For now there is no reason to install the patch because of the closed environment.

3. Performance

We have been testing with an updated Linux kernel and found that the reputed performance impact of these vulnerabilities is almost absent due to the nature of the emulation. This testing is continuing and if we find areas in the future that are affected we will report the impact.

4. OpenVMS or Tru64

The operating systems running on the emulator (OpenVMS or Tru64) are not affected since the emulator does not emulate speculative instruction execution.