Computation slowdown by security updates for the Spectre and Meltdown flaws

March 5, 2018

SES

Historical Perspective

Security researchers discovered late in 2017 that nearly every computer chip manufactured in the last 20 years contains fundamental security flaws, that specialists have called Spectre and Meltdown. The flaws originate from CPU features that help them run faster, and while security updates are now available from Microsoft and Intel, they may have impacts on system performance. Although there is no evidence that these vulnerabilities have been exploited yet, some security analysts consider them as a serious concern.

Spectre and Meltdown are the names given to different variants of the same fundamental uncovered vulnerability referred to as “speculative execution side-channel attacks”.

Before applying the security updates to Windows and the CPU, it is important to know that any compute-intensive application, including our software packages, can be affected depending on how these updates are implemented.

Since the beginning of the year, Windows and CPU security updates have been distributed in order to mitigate the exploits of the recently discovered Spectre (Variant 1, Variant 2) and Meltdown (Variant 3) flaws. Our initial investigation has found that compute-intensive processes may be slowed down tremendously on Windows computers after having installed these security updates.

The security updates encompass the computer’s firmware, BIOS, operating system, and Internet browser. While security updates for Variant 1 and Variant 3 have been documented by Microsoft to have minimal performance impact, the updates to Variant 2 that involves firmware, BIOS, and operating system security updates have been documented to affect the performance.

You may refer to the following webpages of Microsoft, Intel, and AMD in order to verify whether your computer has applied the security updates for these flaws. Additionally, Microsoft has a table on the Windows Protection webpage to locate the update for your computer’s firmware and BIOS via the computer vendor’s site.

Microsoft:

Advisory : https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv180002

Windows Protection: https://support.microsoft.com/en-us/help/4073757/protect-your-windows-devices-against-spectre-meltdown

Windows Server Protection: https://support.microsoft.com/en-ca/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution

Intel: https://newsroom.intel.com/news/latest-intel-security-news-updated-firmware-available/

AMD: https://www.amd.com/en/corporate/speculative-execution

Since the updates of these vulnerabilities are quite recent (January 3, 2018) and the side-effects are emerging to be more prominent and serious than what Microsoft and Intel initially anticipated, a full solution may not be readily available from Microsoft and Intel for the performance degradation as a result of their security updates.

There is abundant information available on the Internet to harness the use of PCID feature (or combinational use with INVPCID) on the affected computer in order to minimize the performance hits. Windows will enable these features by default if the computer's CPU supports them, in which case, the performance impact resulting from these security updates might be mitigated. (Microsoft's SysInternals COREINFO tool can be used to determine the status of the PCID and INVPCID usage by Windows.) Microsoft has released a PowerShell script for comprehensive assessment of protection against the three documented variant flaws: https://support.microsoft.com/en-ca/help/4074629/understanding-the-output-of-get-speculationcontrolsettings-powershell.

In the interim period, until a satisfactory solution has been officially provided by Microsoft and Intel, you may want to evaluate the risk for your environment and balance the security versus performance trade-off if compute-intensive processes have been drastically affected by these security updates.

In conclusion, SES Software has not introduced any vulnerabilities in Version 16.0 that may result in computation slowdown. You should have your IT do the assessment and consult with Microsoft and Intel for an optimum solution.