FAQ on the Meltdown and Spectre Vulnerabilities and the impact to Telestream software

The Meltdown and Spectre vulnerabilities impact many Intel, AMD and RISC processors. A description of what these vulnerabilities can do and what hardware and operating system software vendors are doing to address them can be found at the link below:

https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-heres-what-intel-apple-microsoft-others-are-doing-about-it/

This notice is to provide information that Telestream customers should be aware of with respect to patching systems that may be vulnerable to these issues.

Q – Is Telestream software impacted by these vulnerabilities?
A – The actual vulnerabilities are due to hardware issues. Microsoft and other operating system vendors are taking steps to patch their operating systems to prevent the vulnerabilities from affecting other applications running on vulnerable hardware.

Q – Is Telestream Hardware, like Lightspeed servers, impacted by these vulnerabilities?
A – There is a good likelihood that Lightspeed servers are impacted by the vulnerabilities, as all models utilize Intel processors. The link below includes Intel's recommendations and additional information:
https://newsroom.intel.com/news/intel-responds-to-security-research-findings/

Q – Should I patch Lightspeed and other hardware that is running Vantage or other Telestream software?
A – In accordance with Telestream's recommended Vantage hardware operating system patching practices, it is recommended that customers patch systems as soon as the operating system updates become available.

For reference, below is our recommended OS patching practice, for systems running Vantage:
Telestream encourages that users install Windows updates as soon as they become available. However, we recommend that System Administrators not have "Auto-Update" enabled; rather, we recommend that the update mode be set to "Download When Available", then the system administrator would simply schedule the appropriate "downtime" and apply the updates during this time. If "Auto Update" is enabled, please be aware that an update, applied automatically, and which reboots the machine could lead to lost Vantage jobs (or the necessity to restart jobs).

As always, check with your operating system vendor or system manufacturer and apply any available updates as soon as they are available. Following good security practices that protect against malware in general will also help protect against possible exploitation until updates can be applied. Telestream does not take responsibility for any lost work or functionality due to operating system patching.

Q – Will Telestream software experience a "performance hit" on patched systems?
A – This is unknown at this time, but Telestream will perform comparative benchmarking on non-patched versus patched systems as soon all patches are available. This document will be updated to reflect those results.

Q – Is Telestream Cloud impacted by these vulnerabilities?
A – When Amazon, Microsoft, and Google upgrade their operating system, our cloud deployments are automatically migrated to the new environment. Telestream Cloud users should see minimal impact at this time.

Support questions can be directed to support@telestream.net
Sales questions can be directed to enterprisesales@telestream.net

