Product Notification
CSB #119

To: Sensitech Customers
From: Client Services
Date: 24 January 2018
Re: ColdStream hosted environment: Spectre and Meltdown Vulnerability

---

Reason for Notification

Sensitech Inc. takes the security of our customers' data very seriously. Our ColdStream® hosted solution is implemented as virtual machines within a dedicated cloud environment. In addition, our infrastructure supplies additional protection through a well-defined physical firewall, whereas shared public clouds usually only have a static, non-filtered physical front end. Our dedicated environment is designed to limit risks from all external issues and reduces the overall risk of Spectre and Meltdown.

That said Sensitech is conducting ongoing analyses with our infrastructure provider, RackSpace, to identify vulnerabilities within our production environment specifically related to Spectre and Meltdown. At this time, the following components are identified as requiring intervention:

- **Windows OS**: virtual and physical machines - patches available from the vendor, testing in process
- **SAN storage**: waiting on fix from vendor
- **Hypervisors**: testing in process; will also require system outage to be coordinated with customers

Rackspace has begun to rollout Microsoft OS patches to customers' virtual machines. Testing showed issues between various anti-virus software, which needs to be resolved before the rollout could take place.

The testing process continues. While some vendors have released patches, there have been cases where testing shows negative impact to other areas of the system requiring remediation (e.g., anti-virus). Other vendors have not released their patches as yet (e.g., SAN storage).

Additionally, during initial assessment, we determined there could be a considerable performance impact with several of these fixes, and as a result, additional analysis is required.
Finally, the Rackspace assessment is ongoing and we expect additional information when their assessment is complete.

Our plan is to address all of the known vulnerabilities with minimal impact to customers. The top priority right now is to apply the OS patches, recently released by Microsoft, to our virtual machines. We have started pushing these patches to our Test environments to assess any potential performance impact and pending positive results, we will proceed with deploying the patches to the Production systems. Per Microsoft, there are multiple variables that affect the performance of these mitigations, ranging from the CPU version to the running workloads. In some systems, the performance impact will be negligible, and in others it will be considerable.

This is a complex and evolving situation. While we can't currently offer a timeline when full mitigation and remediation will be complete, we can provide updates when we have relevant new information to share.