Customer Support Bulletin 20180106
Processor Speculative Execution Security Vulnerabilities: Spectre and Meltdown
Product Security Advisory

Industry Concern

Many modern processors may be susceptible to processor speculative execution security vulnerabilities referred to as Spectre and Meltdown. Information on these vulnerabilities has been widely communicated across the technology landscape.

Violin Products

Violin Systems V6000 series and V7000 series Flash Storage Platform (FSP) are closed systems that utilize Intel CPUs. Violin arrays do not enable third party applications to be deployed on these systems. Although we are continuing to monitor developments regarding Spectre and Meltdown, to our knowledge, Spectre and Meltdown vulnerabilities are not exploitable on Violin arrays.

Symphony is a closed software application deployed as a VMware virtual machine. Customers should work with their host system vendors to assess product security and needed remediation.

Violin will continue to monitor the industry's (CPU, OS and Security vendors) technical communications and will assess solutions and apply them as appropriate.

For assistance or questions, please contact Violin Memory Customer Support at https://www.violin-systems.com/services/support-services/

We appreciate your business and continued trust in Violin.

References

- Spectre (CVE-2017-5753/CVE-2017-5715)
- Meltdown (CVE-2017-5754)