Silver Peak Security Advisory

Notification

Microarchitectural Data Sampling (MDS) vulnerabilities

INTEL-SA-00233 originally published by Intel on May 14, 2019

CVE IDs:

CVE-2018-12126	Microarchitectural Store Buffer Data Sampling
CVE-2018-12130	Microarchitectural Fill Buffer Data Sampling
CVE-2018-12127	Microarchitectural Load Port Data Sampling
CVE-2019-11091	Microarchitectural Data Sampling Uncacheable Memory

Summary

MDS is a sub-class of previously disclosed speculative execution side channel vulnerabilities and is comprised of four associated techniques. In this regard, MDS is similar to previously reported variants like L1 terminal fault, meltdown and spectre. Silver Peak hardware products use Intel processors that are susceptible to these vulnerabilities. According to Intel, practical exploitation of MDS is a very complex undertaking. MDS, by itself, does not provide an attacker with the means to select the data that could be obtained unassisted. As it applies to other side channel attacks, per the CERT KB VU#584653, "Single-user systems that do not readily provide a way for attackers to execute code locally face significantly lower risk". Silver Peak hardware products utilize embedded systems that satisfy this criterion. Therefore, the risk associated with Silver Peak deployments presents Low to No-risk. Further, Silver Peak is continuing to work with our manufacturers to update microcode and BIOS on our hardware platforms to eliminate the possibility of vulnerability.

For cloud services hosted by Silver Peak, namely Orchestrator-as-a-service, Orchestrator^{SP} and Cloud Portal, Amazon has already patched EC2 and relevant services.

Applicability to Silver Peak deployments: Low to None

Silver Peak VXOA release for NX/CPX/EdgeConnect appliances is susceptible to this vulnerability, but the applicability is Low to None.

Silver Peak Cloud Services - Orchestrator-as-a-service, Orchestrator^{SP} and Cloud Portal are susceptible to this vulnerability and are already patched.

Silver Peak Virtual Devices – EC-V, VX, VRX, Orchestrator/GMS. Applicability is Low to None for the guest OS. Updates to the underlying physical server platform BIOS/OS are to be evaluated by the respective IT administrators.

Silver Peak cloud-hosted EC-V, VX (IAAS services): Please refer to your cloud provider.

Recommended Action for Silver Peak Customers:

Evaluate physical host, hypervisor security for virtual devices.

VSphere ESXi updates: https://kb.vmware.com/s/article/68024
KVM updates: https://access.redhat.com/security/vulnerabilities/mds

Resolution:

None

References:

The full details of the advisory and the vulnerabilities are found at-

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html

Thank you.

Product Security Incident Response Team

Silver Peak