Silver Peak Security Advisory

Notification

Speculative Execution Side Channel Attacks Update: L1 terminal Fault (L1TF)

INTEL-SA-00161 originally published by Intel on August 14, 2018

CVE IDs:
CVE-2018-3615 - L1 Terminal Fault: SGX
CVE-2018-3620 - L1 Terminal Fault: OS/SMM
CVE-2018-3646 - L1 Terminal Fault: VMM

Summary:

Security researchers have identified a speculative execution side-channel method called L1 Terminal Fault (L1TF). This method impacts select microprocessor products supporting Intel® Software Guard Extensions (Intel® SGX). Further investigation by Intel has identified two related applications of L1TF with the potential to impact additional microprocessors, operating systems, system management mode, and virtualization software. If used for malicious purposes, this class of vulnerability has the potential to improperly infer data values from multiple types of computing devices.
L1TF is a speculative execution side channel cache timing vulnerability. In this regard, it is similar to previously reported variants like meltdown and spectre. Silver Peak hardware products use Intel processors, which are susceptible to these vulnerabilities. But, 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”. This applies to Silver Peak hardware products, which are embedded systems that fall into this category. Therefore, we have determined the applicability to Silver Peak deployments as Low to None. However, we will continue to monitor microcode and BIOS updates from our manufacturers.

For cloud services hosted by Silver Peak, namely Cloud Orchestrator, Orchestrator^{SP} and Cloud Portal, Amazon has already patched EC2 and relevant services. The cloud services have several layers of architectural security implemented around them, which lowers the attack surface. Hence we have determined the applicability to Silver Peak deployments as Low to None. However, the cloud images from Ubuntu are available so we will still patch our cloud servers in the next few weeks.

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 - Cloud Orchestrator, Orchestrator^{SP} and Cloud Portal are susceptible to this vulnerability, but the applicability is Low to None.

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): Applicability is Low to None for the guest OS. For cloud platform updates, please refer to your cloud provider.

Recommended Action for Silver Peak Customers:

Evaluate physical host, hypervisor security for virtual devices.

VSphere ESXi updates: https://vinfrastructure.it/2018/08/l1-terminal-fault-l1tf-vmware-vsphere-patches/
KVM updates: https://access.redhat.com/security/vulnerabilities/L1TF

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-00161.html

Thank you.

Product Security Incident Response Team

Silver Peak