Silver Peak Security Advisory

Notification

CPU Side-Channel Attacks

Spectre Attacks: Exploiting Speculative Execution

Meltdown: Rogue Data Cache Load

VU#584653 originally published by CERT on January 3, 2018

CVE IDs:
Variant 1 (CVE-2017-5753, Spectre): Bounds check bypass
Variant 2 (CVE-2017-5715, also Spectre): Branch target injection
Variant 3 (CVE-2017-5754, Meltdown): Rogue data cache load, memory access permission check performed after kernel memory read

Summary:

This is a TLS security advisory for VU#584653.

CPU hardware implementations are vulnerable to side-channel attacks referred to as Meltdown and Spectre. These attacks are described in detail by Google Project Zero and the Institute of Applied Information Processing and Communications (IAIK) at Graz University of Technology (TU Graz). See *References* below.

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://www.vmware.com/security/advisories/VMSA-2018-0004.html
VSphere ESXi updates: https://www.vmware.com/security/advisories/VMSA-2018-0002.html
Xenserver updates: https://support.citrix.com/article/CTX231390
RedHat KVM: https://access.redhat.com/security/vulnerabilities/speculativeexecution

Resolution:

None

References:

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

https://www.kb.cert.org/vuls/id/584653
https://spectreattack.com/spectre.pdf
https://meltdownattack.com/meltdown.pdf
https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html

Thank you.

Product Security Incident Response Team

Silver Peak