Silver Peak Security Advisory

Release Notification

TCP SACK Panic and other remote denial of service vulnerabilities

NFLX-2019-001 originally published by Netflix on June 17, 2019

Summary

Netflix has identified several TCP networking vulnerabilities in FreeBSD and other Linux kernels.

The vulnerabilities specifically relate to the Maximum Segment Size (MSS) and TCP Selective Acknowledgement (SACK) capabilities. The most serious, dubbed "SACK Panic," allows a remotely-triggered kernel panic on recent Linux kernels.

Silver Peak products are susceptible to these vulnerabilities for self-traffic or traffic destined to the appliance, Orchestrator or respective device. Traffic passing through the appliance is not affected by these vulnerabilities in the Silver Peak environment.

Mitigation

Continue to use our hardening best practices for all Silver Peak appliances and Orchestrators. Deploy EdgeConnect WAN interfaces in 'hardened' or 'stateful firewall' mode (with or without NAT). Allow LAN and management interfaces access from trusted networks. Most system services like SSH, FTP are turned off by default on the EdgeConnect. Since the attack surface can be restricted, applicability to Silver peak deployments is medium.

Applicability to Silver Peak deployments:

Applicable CVEs:

CVE-2019-11477	SACK Panic	Applicable
CVE-2019-11478	SACK Slowness or Excess Resource Usage	Applicable
CVE-2019-5599	SACK Slowness	Not Applicable
CVE-2019-11479	Excess Resource Consumption Due to Low MSS Values	Applicable

Applicable products:

Silver Peak product(s)	**Applicable level**
Unity EdgeConnect, NX, VX	**Medium**
Unity Orchestrator	**Medium**

EdgeConnect in AWS, Azure, GCP	**Medium**
Silver Peak Cloud Services	**Low[1]**

1: Applicability to cloud services is low because they are protected by load balancers that terminate TCP and the load balancers are already patched.

Recommended Action for Silver Peak Customers:

It is recommended to upgrade Silver peak appliances to the below mentioned releases and re-install new Orchestrator images based on the following releases to mitigate risk against the vulnerabilities.

Resolution

The following Silver Peak defect IDs track the fixes: **VXOA-49466, GMS-15090, VXOA-49469, VXOA-49470, DEV-261.**

CVE IDs	Appliance Release	Orchestrator Release
CVE-2019-11477	**Silver Peak VXOA release 8.1.9.5+ , 8.1.7.19+**	**Orchestrator release 8.7.0***
CVE-2019-11478	**Silver Peak VXOA release 8.1.9.6+, 8.1.7.19+**	**Orchestrator release 8.7.0***
CVE-2019-5599	**Not Applicable**	**Not Applicable**
CVE-2019-11479	**Silver Peak VXOA release 8.1.9.5+, 8.1.7.19+**	**Orchestrator release 8.7.0***

*A simple upgrade does not fix the issue for Orchestrator. Install from the new 8.7.0 OVA, QCOW2 or other image.

Patches are in progress for:

Silver Peak IaaS images for EC-V in AWS, Azure, GCP

Patching is in progress for:

Silver Peak Cloud Services - Orchestrator-as-a-service, Orchestrator[SP] and Cloud Portal

References:

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

https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001.md

Thank you.

Product Security Incident Response Team

Silver Peak