# Silver Peak Security Advisory

**Pre-Release Notification**

**OCSP Status Request extension unbounded memory growth (CVE-2016-6304) published by OpenSSL on Sep 22, 2016 - Severity: High**

**Fix Use After Free for large message sizes (CVE-2016-6309) published by OpenSSL on Sep 26, 2016 - Severity: Critical**

## Summary:

This is an OpenSSL security advisory for CVE-2016-6304 and is dated Sep 22, 2016

A malicious client can send an excessively large OCSP Status Request extension. If that client continually requests renegotiation, sending a large OCSP Status Request extension each time, then there will be unbounded memory growth on the server. This will eventually lead to a Denial Of Service attack through memory exhaustion. Servers with a default configuration are vulnerable even if they do not support OCSP. Builds using the "no-ocsp" build time option are not affected.

In fixing CVE-2016-6304, another issue was introduced, so openssl update CVE-2016-6309, dated Sep 26, 2016 states that:

This security update addresses issues that were caused by patches included in our previous security update, released on 22nd September 2016. Given the Critical severity of one of these flaws we have chosen to release this advisory immediately to prevent upgrades to the affected version, rather than delaying in order to provide our usual public pre-notification.

**A device is vulnerable to CVE-2016-6304 if it:**

- Supports OSCP requests processing
- Has a default configuration even if it does not support OSCP

**A device is vulnerable to CVE-2016-6309 if it:**

- Uses OpenSSL 1.1.0a

**Silver Peak Unity Orchestrator/GMS is NOT susceptible to these vulnerabilities.**

**Silver Peak VXOA release is susceptible to CVE-2016-6304 and NOT CVE-2016-6309.**

**Applicability to Silver Peak deployments:** Medium

## Recommended Action for Silver Peak Customers:

**Silver Peak GMS / Unity Orchestrator:**
Silver Peak GMS/Unity Orchestrator is not affected by both the vulnerabilities.

**Silver Peak VXOA release for NX/VX/VRX/CPX/EdgeConnect appliances:**
It is recommended to upgrade Silver peak NX/VX/VRX/CPX/EdgeConnect to the below mentioned releases to mitigate risk against the vulnerabilities. The patches are in line with the recommendations in the CVE-2016-6304 security advisory.

## Resolution:

**Silver Peak Issue Id 32643 tracks the vulnerabilities.**

**The Resolution for this vulnerability will be in each of the below mentioned branches of release:**

**Silver Peak VXOA release 8.1.3.0 and later**

**Silver Peak VXOA release 8.0.6.0 and later**

## Details:

The full details of the advisory are located at-
https://www.openssl.org/news/vulnerabilities.html#y2016

Thank you.

Security Incident Response Team

Silver Peak