Silver Peak Security Advisory

CVE-2014-0160, "Heartbleed Bug"

Summary:

There is an OpenSSL security advisory dated Apr 7 2014 – "TLS heartbeat read overrun", CVE-2014-0160, also known as the "Heartbeat Bug" or "Heartbleed Bug".

Silver Peak customers are not affected by this vulnerability.

Details:

The full advisory from OpenSSL.org, located at https://www.openssl.org/news/secadv_20140407.txt, reads as follows:

```
OpenSSL Security Advisory [07 Apr 2014]
========================================

TLS heartbeat read overrun (CVE-2014-0160)
==========================================

A missing bounds check in the handling of the TLS heartbeat extension can be
used to reveal up to 64k of memory to a connected client or server.

Only 1.0.1 and 1.0.2-beta releases of OpenSSL are affected including
1.0.1f and 1.0.2-beta1.

Thanks for Neel Mehta of Google Security for discovering this bug and to
Adam Langley <agl@chromium.org> and Bodo Moeller <bmoeller@acm.org> for
preparing the fix.

Affected users should upgrade to OpenSSL 1.0.1g. Users unable to immediately
upgrade can alternatively recompile OpenSSL with -DOPENSSL_NO_HEARTBEATS.

1.0.2 will be fixed in 1.0.2-beta2.
```

NIST has added the vulnerability summary for this CVE to their National Cyber Awareness System database:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

According to NIST, remote attackers exploiting the Heartbleed Bug could "obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed Bug."

NIST rates the Heartbleed Bug severity with a CVSS v2 Base Score of 5.0 (MEDIUM). For details on NIST impact ratings, browse to http://nvd.nist.gov/cvss.cfm?vectorinfo&version=2.

Recommended Action for Silver Peak Customers:

The Heartbleed bug is related to handling of TLS heartbeat extension packets and only affects 1.0.1 and 1.0.2-beta releases of OpenSSL, neither of which are in use by any version of Silver Peak VXOA and GMS releases.

Silver Peak products use the following versions of OpenSSL:

Silver Peak VXOA:	OpenSSL 0.9.8b
Silver Peak GX-V (6.0.2 and later):	OpenSSL 1.0.0e-fips
Silver Peak GX-V (pre-6.0.2):	OpenSSL 1.0.0b-fips
Silver Peak GX-1100s:	OpenSSL 1.0.0b-fips

The Heartbleed Bug only affects OpenSSL versions 1.0.1 and 1.0.2-beta.

OpenSSL versions 0.9.8b, 1.0.0e-fips, and 1.0.0b-fips are unaffected.

Silver Peak customers do not need to take any action on their Silver Peak products.