Heartbleed Announcment

Update as of 04.11.2014

As you may have heard, in the last couple of days a security vulnerability was identified called Heartbleed. This vulnerability affects SSL communications that use the popular OpenSSL cryptographic library, and allows stealing of encrypted information.

You can get more info about this vulnerability at http://heartbleed.com/.

We at CrownPeak take security issues very seriously, and have reviewed our systems to determine where this vulnerability might apply. We used the following remediation steps:

- *CrownPeak uses a variety of Amazon Web Services (AWS) technologies, some of which were exposed to the Heartbleed vulnerability. Amazon has taken immediate step described here: http://aws.amazon.com/security/security-bulletins/aws-services-updated-to-address-openssl-vulnerability/*
- *The CrownPeak CMS has been reviewed, patched and remediated in its entirety.*
- *Websites running HTTPS on Apache Web services on Linux machines may be vulnerable if they contain older versions of the OpenSSL libraries. We have patched all Web servers where this vulnerability was discovered.*
- *Please contact CrownPeak Customer Support to determine if you need to replace your SSL certificates.*

At CrownPeak we strive to maintain the highest level of security awareness, and will continue to monitor and react quickly when issues such as these arise. If you have any questions regarding the impact of the Heartbleed vulnerability, do not hesitate to contact us.

CrownPeak™