LifeSize
A division of Logitech

LifeSize Heartbleed Vulnerability Update: April 18, 2014

The "Heartbleed Bug" is a vulnerability related to secure communications (SSL) that was discovered on April 7, 2014. The Heartbleed website has many more details on the issue.

The vulnerability is associated with the open-source secure communications library known as OpenSSL.

The status of the various OpenSSL versions is as follows:

- OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
- OpenSSL 1.0.1g is NOT vulnerable
- OpenSSL 1.0.0 branch is NOT vulnerable
- OpenSSL 0.9.8 branch is NOT vulnerable

LifeSize products affected:

- The general assessment related to this bug is that the only confirmed products with vulnerability are LifeSize® UVC ClearSea™ Server (CSS) and LifeSize® ClearSea™ Client (CSC).
- LifeSize has verified that all video systems (Icon, 220s, 200s, Unity, LG, Passport, etc), bridges and other UVC components are NOT vulnerable.

Current status on fixed versions:

- A software patch for LifeSize UVC ClearSea Server (v.4.0.4), which includes the desktop LifeSize ClearSea clients v. 8.2.10 (Mac/PC) is available for download on software.lifesize.com.
- Although LifeSize® ClearSea™ Server wasn't affected by the Heartbleed vulnerability we recommend upgrading to version 3.1.6 which includes the Desktop Client (v. 8.2.10). LifeSize ClearSea v. 3.1.6 is available for download on software.lifesize.com.
- LifeSize ClearSea Mobile Client v. 8.2.10 is available for download on Google Play for Android™ devices, on the Amazon Appstore for Android for Kindle Fire™ HD and on the Apple App Store for iOS devices.

If you have any further questions or concerns, please send us an email at support@lifesize.com and a customer support representative will contact you shortly.

Best regards,
LifeSize Support Team