Customer Notification

For further information contact:

Paul Barnes, Marketing Manager – Icomera

+46 (0)31 799 21 00

paul.barnes@icomera.com

Icomera Moves Quickly to Eliminate Heartbleed Vulnerability

April 14th 2014 - Following the public disclosure of the existence of the Heartbleed bug in early April, Icomera wishes to reassure our customers that immediate action was taken to eliminate any vulnerabilities that may otherwise have been exploited.

Heartbleed is an OpenSSL security bug allowing hackers to steal information that should usually be protected by SSL/TLS encryption. OpenSSL is used to protect the browser traffic to and from as many as two thirds of all servers on the Internet. The Heartbleed bug exposes a hole in an OpenSSL extension called "heartbeat" which allows web servers to keep secure connections open over a longer period of time.

The existence of the bug was publicly disclosed on April 7th 2014, at which point all vendors started to prepare and distribute patches for it. By April 9th the approved security patches had been applied to all of Icomera's affected servers and appropriate action was taken regarding certificates.

At no point were Icomera's customers or their data directly at risk and customers are not required to take any additional action themselves. The main area of vulnerability was that Heartbleed would have potentially allowed unauthorized parties to impersonate Icomera https.

Icomera remain committed to protecting our customers' data and in the rare cases where major online security issues do arise, please be assured that our ever-vigilant team will be on hand to combat these swiftly and decisively.

Customers with any outstanding questions or concerns should contact their Icomera account manager.

For more information about Heartbleed please visit heartbleed.com.