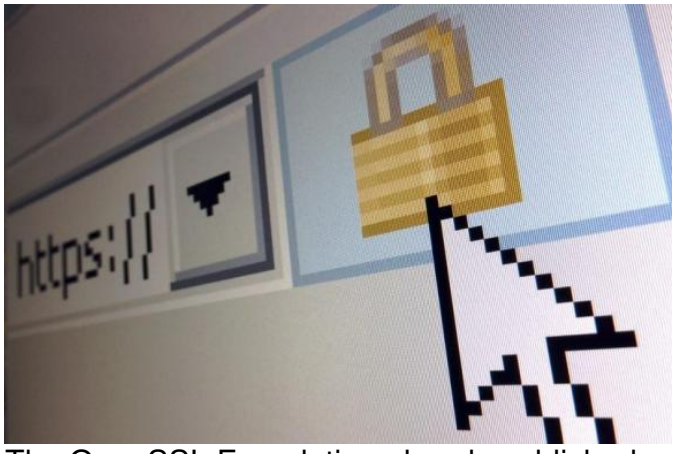
Written by Marco Attard
06 June 2014

Mere months after the discovery of the Hearthbleed vulnerability , the entity behind the widely used OpenSSL encryption software issues a warning of another security vulnerability.



The OpenSSL Foundation already published an advisory asking users to yet again update their SSL.

Discovered by Japanese researcher Masashi Kikuchi, the new vulnerability involves ChangeCipherSpec (CCS), a portion of the OpenSSL "handshake" procedure. Dubbed "CCS Injection Vulnerability," it allows attackers to force a PC and server to use weak encryption keys as they handshake, opening the systems for "man-in-the-middle" snoops to decrypt and read traffic.

According to Kikuchi the bug has been in OpenSSL for over 16 years, and was caused by insufficient code reviews. Technically it is not as nasty as Heartbleed (thus the lack of catchy name), but still it impacts many internet users, especially those taking advantage of anonymity tools such as ToR.

Either way, make sure your customers get patched up asap, especially when it comes to web servers and systems using SSL encryption. After all, as we said back when Heartbleed made its first appearance, in this case it's the cleaners who get paid and be heroes.

Go OpenSSL Security Advisory

Go How I Discovered CCS Injection Vulnerability