El personal de JAVACOL presenta un saludo cordial a todos los clientes que cuentan con nuestros servicios.

Según los informes de las diversas organizaciones encargadas de la seguridad en la Internet, les podemos comunicar a nuestros clientes, que los constantes informes sobre el error de seguridad "Heartbleed" **NO AFECTA A LOS USUARIOS DE JAVACOL.**

El bug de seguridad se encuentra en una librería de OpenSSL en las versiones 1.0.1 a 1.0.1f y los servidores de JAVACOL usan OpenSSL 0.9.8e-27 del cual, hasta el momento **NO** se han informado problemas de seguridad.

Si desea comprender más la problemática que se generó a raíz de este inconveniente, se traen apartes de dos artículos que presentan una explicación clara sobre el tema.

¿Qué es el bug Heartbleed?

El conocido como bug Heartbleed hace referencia a un fallo resultante de una filtración de datos inesperada.

El problema del fallo viene porque éste provoca un comportamiento imprevisto debido a un error en la codificación del proceso en la librería OpenSSL, la encargada de una comunicación segura usada para procesos bancarios, redes sociales o tiendas *online*, es decir, el famoso candado que se ve delante de algunas URLs.

Con esto se permitiría a un atacante recuperar las claves privadas y, finalmente, descifrar el tráfico cifrado del servidor o incluso hacerse pasar por el propio servidor. [1]

[1] http://www.eleconomista.es/tecnologia-internet/noticias/5697100/04/14/Que-es-el-bug-Heartbleed-y-por-que-deberia-cambiar-sus-contrasenas-de-Internet.html

¿Qué es el bug Heartbleed exactamente?

Su nombre real es poco sugerente: **CVE-2014-0160**, un número de catálogo. El apodo de *Heartbleed* ('el corazón que se desangra') hace referencia a que el fallo en cuestión es una filtración de datos inesperada -cual desangramiento- en el corazón de un servidor de Internet, las máquinas a las que nos conectamos mientras navegamos.

Fue descubierto hace poco por Neel Mehta del departamento de seguridad de Google, quien -como *hacker bueno* y tal y como se recomienda en estos casos- avisó a los responsables para que prepararan una solución antes de darlo a conocer al público en general.

El problema en cuestión es un bug, un comportamiento imprevisto debido a un error en el código. ¿En qué parte del código exactamente? En una zona o librería llamada **OpenSSL** presente en algunos servidores web que es la que se encarga de las comunicaciones confidenciales y seguras, el famoso "candadito" que puede verse en la barra de navegación y que se activa cuando se visitan tiendas, bancos o redes sociales.

OpenSSL también sirve para garantizar (mediante algo llamado "certificado") que cada web es quien dice ser y otras cuestiones importantes, especialmente para los negocios en la red. Y otro detalle importante es que aunque no todos los servidores de Internet utilizan OpenSSL -pues existe software alternativo- se han cifrado en cientos de miles de servidores los afectados, entre ellos muchos de los más populares.

El bug en cuestión se produce debido a cómo se gestiona algo llamado 'extensión Heartbeat', una especie de señal en forma de 'latido' que se emplea para sincronizar procesos, servidores y asegurarse de que todo funciona correctamente. [2]

[2] http://heartbleed.com/