# Heartbleed revuelve Internet


Seguramente estáis al tanto de lo que fue noticia en materia de seguridad informática: una vulnerabilidad en OpenSSL que afectaría a **dos de cada tres servidores del mundo que hacen uso de OpenSSL** y que algunos expertos califican como la de mayor gravedad en la historia de Internet.

En esencia, lo que propiciaba el agujero, al que han denominado Heartbleed en relación a una función concreta de OpenSSL, era la **vulneración total del sistema de cifrado** que utiliza una gran parte de las transmisiones en línea supuestamente seguras. De hecho, hasta una página web dedicada han abierto para dar información a administradores de sistemas y usuarios interesados.

Sin embargo, lo más curioso y grave del asunto no es el descubrir una vulnerabilidad de semejante calibre que ha sido parcheada con "rapidez" -así es como funciona el desarrollo de software-, sino conocer que la misma está **presente en computadoras en producción de todo el mundo desde hace casi un año**.

Para más datos acerca de Heartbleed, las anteriores fuentes y cien más que encontraréis por toda la Red, aunque si preferís una explicación sencilla y certera, la que publica hoy Chema Alonso en su blog.

Como usuarios lo único de lo que os debéis preocupar es de **actualizar vuestros sistemas**, que ya han distribuido la actualización con el parche de rigor -me refiero a Linux, claro-, y como medida excepcional, **cambiar todas vuestras contraseñas de sitios web…** Porque se desconoce si el agujero

ha sido explotado.

Y aquí es donde esta entrada vira ligeramente, pues hablamos una vez más en poco tiempo de un **error grave en un componente crítico de seguridad de código abierto**. Ante sucesos como este, alguien sin los conocimientos necesarios como para comprender los pormenores técnicos pero con algo de audacia se podría preguntar: ¿cómo un error de tal envergadura ha pasado desapercibido durante tanto tiempo? ¿Podría ser un error intencional? ¿Ha sido explotado? ¿Cuántos habrá como éste de los que no se sabe nada?

Así, cuando decimos en MuyLinux que el software libre es intrínsecamente más seguro que el privativo, es porque así lo consideramos. Del mismo modo, cuando decimos que Linux o **cualquier proyecto de software libre de cierto nivel no está exento de problemas de este tipo**, es porque así lo consideramos. Porque a estas alturas de la vida ya no te puedes fiar de nada y porque lo que en algunos casos -la mayoría, suponemos / esperamos- puede ser, efectivamente, una vulnerabilidad, en otros podría tratarse de una puerta trasera sin que nunca nos diésemos cuenta.

Dicho de otra forma, el software libre, por su modelo de desarrollo abierto, siempre será más seguro. Pero **estamos en la era de Internet y las reglas del juego han cambiado**, y tan perjudicial es despotricar contra el software libre, como creerse a salvo de todo mal por utilizar software libre.

fuente:humanos.uci.cu