LibreSSL Portable Aparece Como El Futuro Sucesor De OpenSSL

La vulnerabilidad que se encontró en OpenSSL generó cierto revuelo, y no es para menos. Como bien se sabe, la mayoría de los sistemas informáticos que manejan información personal de los clientes usan este certificado de seguridad. Después de haberse anunciado el descubrimiento de HeartBleed, se ha cuestionado el nivel de seguridad que brinda OpenSSL a los sitios web, es por esto que se ha pensado en desarrollar otro certificado de seguridad que vuelva a brindar esa confianza a los usuarios. El pasado fin de semana la Fundación OpenSSL ha liberado el paquete LibreSSL portátil, un fork que permitirá ademas de confianza, características como el concepto de multiplataforma.

El lanzamiento de la versión 2.0.x de LibreSSL es el primero en soportar oficialmente otro Sistemas Operativos distintos de OpenBSD, con «varias versiones» de Linux, Solaris, Mac OS X y FreeBSD que ahora son soportados. «Esto versión inicial pretende permitir a la comunidad el uso y proporcionar información», dijo el director de la Fundación OpenBSD y desarrollador de OpenBSD **Bob Beck**. «Vamos a añadir soporte para otras plataformas con el tiempo, siempre y cuando los recursos económicos lo permitan».

Mientras que la biblioteca se ha ganado el apoyo para nuevos sistemas operativos, aún no está listo para ser el reemplazo de OpenSSL, pero sin duda alguna, la **fundación de OpenSSL** tiene la intención de que sea así. El desarrollador de Gentoo Johannes «Hanno» Böck detalla el proceso de cambiar OpenSSL a LibreSSL.

Böck dijo que el tema más interesante que encontró fue el desarrollo de OpenSSL que la dependencia de LibreSSL en OpenSSL, a pesar de que ambos están desarrollados para OpenBSD. «Para entender esto hay que entender cómo se desarrollan tanto LibreSSL y OpenSSH», escribió Böck. «Los dos son de OpenBSD y **utilizan algunas funciones que sólo están disponibles allí**. Para permitir que se desarrollen para otros sistemas que liberan versiones portátiles que enviarán a las desaparecidas funciones de OpenBSD. Uno de ellos es **arc4random ()**.»

La revisión que Böck ha encontrado era copiar a través de los archivos de arc4random.c OpenSSL para LibreSSL «sorprendentemente bien», y después de una serie de otras correcciones y parches, fue capaz de tener un sistema de prueba que utiliza sólo LibreSSL.

El equipo de OpenBSD tomó la decisión de dar la oportunidad a un **nuevo y mejorado certificado de seguridad**, el cual llamaron LibreSSL, luego de ver la vulnerabilidad de HeartBleed. En una actualización del estado del proyecto LibreSSL entregado en mayo, Beck dijo que esta vulnerabilidad no estaba presente en LibreSSL. «Vamos a aplicar nuestra propia caché que nunca libera nada y sólo vuelve a utilizar los objetos. Mejor aún, la forma en que se vuelve a utilizar los objetos es que mantiene una última en la cola, la cual es el primer dato en salir, por lo que si en realidad se está haciendo un uso después de liberación , lo más probable es que ese objeto está todavía allí «.

«De hecho, es casi seguro que si algo es libre y es utilizado de inmediato, ese desarrollo seguirá creciendo, sin importar quien la liberó.» Con este nuevo certificado, se pretende asegurar el uso de la información delicada que se maneja en los servidores, y evitar un futuro ataque como el ya conocido HeartBleed.