Nuevo Bug Encontrado En OpenSSL

Anteriormente conocimos un **bug de seguridad** bastante preocupante en el certifico de seguridad mas usado en el mundo, este bug se le conoció como HeartBleed. Aunque se dio rápidamente una actualización que corregía este fallo de seguridad, el jueves, la Fundación OpenSSL emitió una advertencia a los usuarios, sobre un error de hace diez años, el cual hace posible realizar el famoso ataque man-in-the-middle en el tráfico cifrado con OpenSSL.

Se aconseja a los usuarios de OpenSSL, instalar un nuevo parche y tener la ultima actualización de la versión del software OpenSSL. El error fue descubierto inicialmente por **Masashi Kikuchi**, un investigador japonés en Lepidum, una empresa de software. «Los atacantes pueden interceptar y hacer falsificaciones en su comunicación cuando tanto el servidor y cliente son vulnerables», segun expone en el sitio de FAQ de Lepidum.

A **diferencia de Heartbleed**, que podría ser utilizado para explotar directamente cualquier servidor que utilizara OpenSSL, este nuevo error requiere que el atacante se encuentra entre dos ordenadores que se comunican. Un posible objetivo, sería alguien que use el Wi-Fi publico de un aeropuerto.

El nuevo error, que no es tan nuevo, extiste desde que fue lanzado OpenSSL (en 1998), más de **10 años antes de Heartbleed**, este ultimo se introdujo por primera vez en una actualización en la víspera de Año Nuevo **en 2011**.

El hecho de que este error no fue detectado durante tanto tiempo, es otro punto negro en la gestión de **OpenSSL**. El método de cifrado es de **código abierto**, lo que significa que

su código puede ser estudiado y modificado por cualquier persona. Debido a eso, se considera más seguro y más confiable que el código propietario.

Después que se descubrió **Heartbleed**, grandes empresas, como Amazon, Cisco, Dell, Facebook, Fujitsu, Google, IBM, Intel, Microsoft, NetApp, Rackspace, Qualcomm y VMWare, acordaron cada uno de dar 100.000 dólares al año durante los próximos tres años para la **Core Infrastructure Initiative**, una nueva iniciativa que busca incentivar los sistemas libres a que sean robustos, como **OpenSSL**.