OpenSSL Tiene Una Vulnerabilidad De Seguridad Crítica Que Necesita Ser Parcheada De Inmediato

El proyecto **OpenSSL** sólo ha revelado una falla de seguridad devastadora en el protocolo que podría exponer las claves criptográficas y comunicaciones privadas de algunos de los sitios y servicios más importantes en Internet. Si está ejecutando un servidor con **OpenSSL 1.0.1** mediante 1.0.1f, es vital que **actualice a OpenSSL 1.0.1g** inmediatamente.

Heartbleed.com tiene una explicación detallada del problema, que se relaciona con la capa de la seguridad de transporte de los protocolos **OpenSSL (TSL)**. Esto es aún más peligroso que el reciente fallo **SSL de Apple**, que abrió la posibilidad de ataques de «hombre en el medio», debido a que el error **Heartbleed** afecta al tráfico pasado, revela las claves de cifrado que podrían conducir a otras fallas, y puede afectar tanto como 66 por ciento de los sitios de Internet.

El error fue descubierto independientemente por un ingeniero de seguridad de **Google** y la firma de seguridad **Codenomicon**.

Antes de la publicación de la vulnerabilidad, un número de vendedores de **OpenSSL** fueron notificados de forma privada con el fin de darles tiempo para abordar el asunto antes de que se conociera. Sin embargo, no todo el mundo estaba listo antes de que la noticia se hubiera conocido, por lo que algunos vendedores necesitarán un par de horas para preparar el parche.

-> Fuente