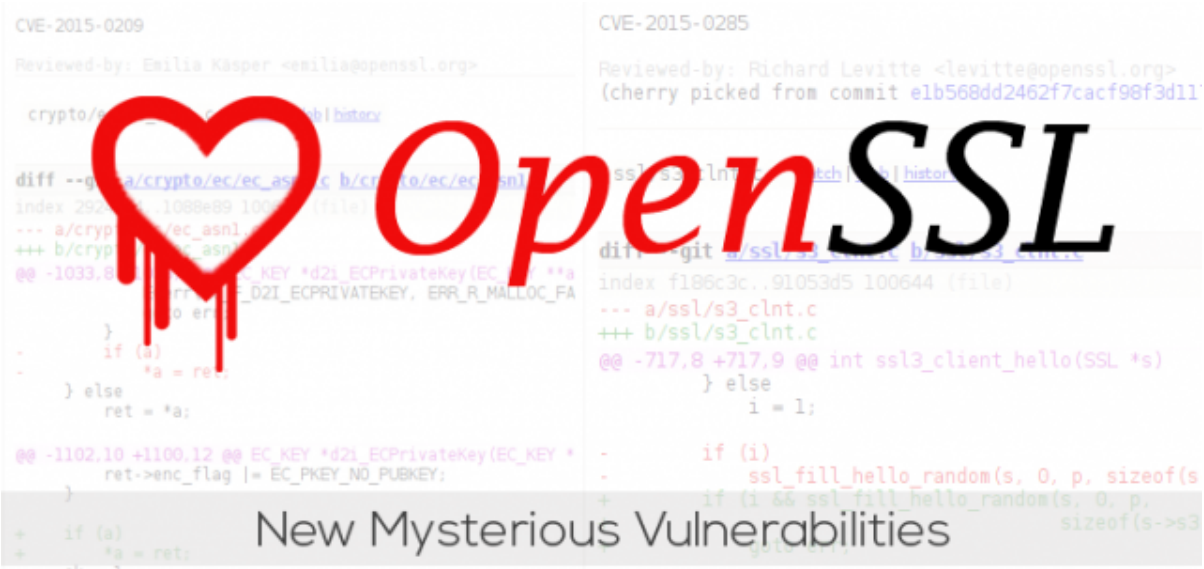
Grave Vulnerabilidad En OpenSSL Ha Sido Descubierta

La Fundación OpenSSL está listo para lanzar un puñado de **parches para vulnerabilidades de seguridad** no reveladas en su software de código abierto ampliamente utilizado, incluyendo uno que ha sido calificado como de «alta» la gravedad.



En una nota de la lista de correo publicada ayer por la noche, **Matt Caswell** del Equipo del Proyecto OpenSSL, anunció que se darán a conocer las versiones 1.0.2a, 1.0.1m, 1.0.0r y 0.9.8zf de OpenSSL.

> *«Estas versiones estarán disponibles el 19 de marzo», escribió Caswell. «Ellos van a solucionar un número de defectos de seguridad. El mayor defecto de seguridad solucionado por estas liberaciones se clasifica como de» alta»gravedad».*

OpenSSL es una implementación de código abierto de los **protocolos SSL y TLS**. Es una tecnología que se utiliza ampliamente en casi todos los sitios web para **cifrar sesiones web**, incluso el servidor web Apache. Heartbleed fue descubierto en abril del año pasado en una versión anterior de

OpenSSL, que permitía a los hackers para leer los contenidos sensibles de datos cifrados de los usuarios, como las transacciones de tarjetas de crédito e incluso robar claves SSL de los servidores de Internet o software de cliente.

Además, en junio de ese mismo año una grave vulnerabilidad Man-in-the-Middle (MITM) fue descubierta y se solucionó por el Equipo del Proyecto OpenSSL. Sin embargo, la vulnerabilidad no era tan grave como la falla Heartbleed, pero es lo suficientemente grave como para descifrar, leer o manipular los datos cifrados, que afectan especialmente a los usuarios de Android.

Casi todas las grandes marcas se vio afectada por la falla FREAK, incluyendo los smartphones Apple y Android, dispositivos BlackBerry y servicios en la nube, así como todas las versiones de sistema operativo Windows. Grandes empresas, como Google, Facebook, y Cisco, están financiando la «Iniciativa de Infraestructura Core», un proyecto de US $2 millones al año.