Masterhacks – Los expertos e investigadores de vulnerabilidades de Google encontraron que el código SSL 3.0 se encuentra vulnerable a ataques de hackers, puesto que posee ciertas características al momento de cifrar los datos que con habilidades informáticas resulta fácil el robo de información.

En un comunicado, Google comentó: “Un atacante de la red puede provocar fallos en la conexión que puede desactivar el uso del SSL 3.0 y luego aprovechar este problema”.

Poodle es el nombre de esta vulnerabilidad, misma que fue encontrada en el mismo protocolo donde se encontró Heartbleed con la que hackers pudieron acceder a información confidencial de usuarios de Facebook, Yahoo y otros sitios más.

Google afirma que la solución más viable es la más fácil, desactivar el cifrado SSL 3.0, mismo que ya es obsoleto pues desde hace 15 años fue sustituido, sin embargo, el día de hoy muchas páginas lo siguen utilizando.

Por otro lado, Google afirmó que desactivará a partir de hoy el código SSL 3 de su navegador Chrome, por lo que varias páginas abiertas desde este navegador aparecerán como fuera de servicio.

De igual forma, Google dejará de dar soporte al SSL 3.0 en cualquiera de sus productos.