La función de seguridad que resguarda la confidencialidad de tu comunicación web (el mismo *software* de criptografía afectado recientemente por la falla Heartbleed) tiene más problemas.

Y a esta nueva vulnerabilidad podemos llamarla *handshake bug* o “la falla del apretón de manos”.

Los ordenadores y servidores web entablan conversaciones seguras entre sí en un proceso conocido como *handshake*. Pero esta semana, los investigadores de seguridad descubrieron un problema en la forma en que ‘se dan la mano’ o establecen esa conexión. La falla permite que un*hacker* que opera entre el usuario y un sitio web -por ejemplo, alguien conectado a la misma red pública WiFi- fisgonee tu sesión de Internet.

Esta falla no es tan devastadora como Heartbleed. Los únicos navegadores importantes a los que afecta son los del sistema operativo móvil Android de Google. Y para que un *hacker* explote esa grieta, tú y el sitio web deben estar ejecutando versiones vulnerables del *software* de encriptación, conocido como OpenSSL.

Aunque no es tan grave, es otra llamada de atención que delata que tu seguridad en Internet depende de un puñado de personas sin sueldo. La Fundación OpenSSL es un pequeño equipo de programadores informáticos que apenas recientemente comenzaron a recibir apoyo financiero adicional de muchas empresas que usan ese *software.*

La Fundación Linux dijo que OpenSSL ha recibido alrededor de la mitad de los 5.4 millones de dólares que hasta la fecha han donado las empresas a la Core Infrastructure Initiative, una iniciativa que busca mejorar la seguridad en Internet.

De hecho, muchos expertos dicen que la única razón por la que pudo detectarse la falla Handshake es porque, después de Heartbleed, más voluntarios están peinando exhaustivamente el código informático OpenSSL. El mundo puede darle las gracias a Masashi

Kikuchi, un experto en *software* de seguridad de la pequeña consultora japonesa Lepidum, que decidió revisar el código personalmente.

“La principal razón de que la falla no fuera detectada en 16 años es porque las revisiones de código son insuficientes”, escribió Kikuchi en una entrada de blog.

Artículo relacionado: Oribe Peralta, un peligro… en Internet

La falla ya ha sido corregida, y ahora toca a los fabricantes de navegadores web y a los servidores de sitios web actualizar sus sistemas. Según Adam Langley, un investigador de Google, estos navegadores son seguros:

- Internet Explorer
- Firefox
- Chrome (para escritorio, iOS)
- Safari

De acuerdo con el director de ingeniería de Qualys Ivan Ristic, estos navegadores son vulnerables:

- Android
- Chrome (para Android)

“No debería causarnos sorpresa que haya más fallas en OpenSSL”, señaló Jean Taggart, un investigador de Malwarebytes, fabricante de antivirus. “La seguridad es un proceso, no un producto”.

Si te preocupa el *bug*, la mejor manera de evitarlo es mantenerse limpio: no usar la WiFi de extraños.

Fuente: cnnexpansion