Suites de TLS/SSL (Parte III)

Por mikiminoru el 21 sept 2020 con 0 comentarios

Siguiendo con este hilo, vamos a enumerar y describir las vulnerabilidades más conocidas que nos encontramos asociadas a los protocolos y algoritmos usados en las suites de cifrado. En este post trataremos la primera mitad de este conjunto de vulnerabilidades.

BEAST (Browser Exploit Against SSL/TLS) - CVE-2011-3389

- Descripción:
  - Permite realizar ataques MiTM para obtener información de una sesión que usa SSL/TLS1.0.
  - Esta vulnerabildad es muy compleja de explotar ya que necesita realizar fuerza bruta para conseguir información útil.
  - Es originada por los vectores de inicialización de TLS1.0 en los cifrados de CBC y RC4.

- Recomendación: Deshabilitar SSLv3, TLS1.0 y TLS1.1 en el servidor.

CRIME (Compression Ratio Info-leak Made Easy) - CVE-2012-4929

- Descripción:
  - Se basa en el secuestro de sesiones en los protocolos HTTPS y SPDY a través del robo de las cookies de sesión, explotando la compresión HTTP con fuerza bruta. Esta explotación es posible ya que SSL/TLS y SPDY usan un algoritmo de compresión llamado DEFLATE, que elimina strings duplicadas durante la conexión entre el cliente y el servidor.
  - A pesar de esto, la compresión TLS se encuentra deshabilitada actualmente en los navegadores Chrome, Mozilla, Opera Safari e Internet Explorer, por lo que deshabilitarla en el servidor ayudaría a proteger a aquellos usuarios que usen navegadores desactualizados.

- Recomendación: Desactivar la compresión en TLS y en HTTP en el servidor.

BREACH (Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext) - CVE-2013-3587

- Descripción:
  - Es una variante del ataque CRIME, que se diferencia de éste en que BREACH se centra en el ataque de las respuestas HTTP, las cuales usan la compresión a nivel de HTTP (en vez de a nivel de TLS, como es el caso de CRIME), que a su vez es más común.

- Enlace de referencia de la vulnerabilidad: http://breachattack.com/
- Recomendación: Desactivar la compresión en TLS y en HTTP en el servidor.

FREAK (Factoring RSA Export Keys) - CVE-2015-0204

- Descripción:
  - Se centra especialmente en los servidores que aceptan RSA_EXPORT en sus suites de cifrado.
  - Consiste en interceptar las comunicaciones HTTPS entre el cliente y el servidor, y forzar al servidor a usar cifrados obsoletos o vulnerables (es decir, a hacer downgrade) para romper las claves.

- Enlace de referencia de la vulnerabilidad: https://censys.io/blog/freak
- Recomendación: Deshabilitar RSA_EXPORT y versiones inferiores a TLS1.2

Heartbleed - CVE-2014-0160

- Descripción:
  - Permite que un atacante pueda leer la memoria de un cliente o servidor, pudiendo conseguir las claves privadas de un servidor SSL y comprometiendo tanto la integridad del servidor como la de los usuarios que se conecten al mismo, además de su confidencialidad.

- Enlace de referencia de la vulnerabilidad: http://heartbleed.com/
- Recomendación: Deshabilitar SSL en el servidor.

En el siguiente post continuaremos viendo el resto de estas vulnerabilidades.

Muchos maullidos!

M

MITM , SSL , TLS , VULNERABILIDADES

Otros artículos relacionados

TLS1.3: ¿Qué hay de nuevo? (Parte I)

30 DE OCTUBRE DE 2020

Suites de TLS/SSL (Parte IV)

22 DE SEPTIEMBRE DE 2020

TLS1.3: ¿Qué hay de nuevo? (Parte II)

Suites de cifrado TLS/SSL (Parte II)