Suites de TLS/SSL (Parte IV)

Por mikiminoru el 22 sept 2020 con 0 comentarios

En este cuarto y último post de este hilo vamos a terminar de tratar las vulnerabilidades asociadas a diferentes malas configuraciones en servidores SSL.

Bar Mitzvah - CVE-2015-2808

- Descripción:
  - Explota la generación pseudo-aleatoria de claves que usa el algoritmo RC4, y con ella poder conseguir los 100 primeros bytes de una conexión TLS/SSL.

- Recomendación: Deshabilitar el uso de RC4.

LOGJAM - CVE-2015-4000

- Descripción:
  - Posee una lógica similar a la vulnerabilidad FREAK ya que ambos buscan hacer downgrade al servidor, pero con la diferencia de que en este caso vulnera aquellos servidores que soportan DHE_EXPORT (debido a un fallo en el protocolo TLS) forzándolos a usar un grado menor de exportación en las conexiones de 512bits, el cual puede ser descifrado con relativa facilidad.

- Enlace de referencia de la vulnerabilidad: https://weakdh.org/
- Recomendación: Deshabilitar DHE_EXPORT e implementar Diffie-Hellman 2048-bit.

Lucky13 - CVE-2013-0169

- Descripción:
  - Este ataque es más teórico debido a las condiciones que deben establecerse en la configuración del servidor y el gran número de peticiones que debe realizar, explotando el uso de CBC (Cipher-Block-Chainning) y el cálculo del MAC.

- Recomendación: Deshabilitar el uso de CBC.

POODLE - CVE-2014-3566

- Descripción:
  - Parte de que, cuando un intento de conexión segura falla, se procede a intentar realizar de nuevo esa conexión pero con un protocolo de comunicación más antiguo. De esa forma, un atacante podría ocasionar intencionadamente errores de conexión en protocolos seguros como TLS 1.2, TLS1.1 y TLS1.0 y forzar así el uso de SSL 3.0 para aprovechar la vulnerabilidad.

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

SWEET32 - CVE-2016-2183

- Descripción:
  - Facilitaría que un atacante remoto pueda obtener información confidencial debido a un error en el cifrado DES/3DES.
  - Un atacante podría realizar ataques MiTM con la captura de grandes cantidades de tráfico cifrado entre el servidor SSL/TLS y el cliente, y

recuperar los datos de texto sin cifrar.

- Enlace de referencia de la vulnerabilidad: https://sweet32.info/
- Recomendación: Deshabilitar SSLv3, TLS1.0 y TLS1.1 en el servidor.

RACCOON - CVE-2020-1968

- Descripción:
  - Hace uso del intercambio de claves de Diffie-Hellman durante el handshake en TLS1.2 (y versiones anteriores), de forma que descifra la conexión entre un cliente y el servidor.
  - La vulnerabilidad se encuentra en la clave Premaster Secret usada a la hora de generar las claves de cifrado en la comunicación, la cual se usa como variable de entrada en la KDF (Key Derivation Function). La KDF se basa en hashes con diferentes perfiles de tiempo, de forma que dichas mediciones de tiempo pueden ayudar a un atacante a generar nuevas claves Premaster Secret, reenviando al servidor esta clave para suplantar la identidad de un cliente en una nueva conexión.
  - Este ataque es complejo de explotar, dado que se deben realizar un gran número de peticiones para construir una nueva clave, y a su vez depende de la configuración del *server timing behavior*.

- Enlace de referencia de la vulnerabilidad: https://raccoon-attack.com/
- Recomendación: Deshabilitar el uso de Diffie-Hellman para el intercambio de claves (DH key exchange) en TLS1.2 y versiones inferiores.

Esperamos que con este hilo hayáis comprendido mejor el funcionamiento de las suites de cifrado y las consecuencias más conocidas de sus malas configuraciones en los servidores SSL.