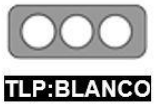

Vulnerabilidad Freak de SSL

(Freak: Factoring RSA Export Keys)

1. INTRODUCCION

FREAK es un fallo de seguridad que hace que los usuarios puedan ser víctimas de ataques informáticos, cuando acceden a algunas webs que utilizan servidores y clientes TLS/SSL vulnerables para gestionar el cifrado de los certificados. La vulnerabilidad afecta a TLS / SSL, el protocolo de seguridad que pemite la navegación segura HTTPS (responsable del candado en la barra de direcciones del navegador).

El reporte entregado identifica a los hosts que permiten el uso de SSL/TLS con cifrado RSA_EXPORT (también conocido como encriptación de “grado de exportación”).

Estas páginas web contienen una vulnerabilidad en la gestión de los certificados que puede ser explotada para obligar a utilizar el certificado en modo “RSA_EXPORT”, técnica utilizada en 1990 para establecer las conexiones seguras, exponiendo la seguridad y la privacidad de los usuarios que se conecten a estas páginas web, incluso las que muestren el candado de seguridad HTTPS.

2. RIESGOS

Los servidores y clientes (navegadores) que utilizan los sistemas de cifrado débiles pueden ser víctimas de un ataque (mitm: man-in-the-middle)) para forzar a un navegador a utilizar un algoritmo de cifrado débil, que pueda ser crackeado. Este ataque es conocido como FREAK (Factoring RSA Export Keys), El atacante forza a utilizar un cifrado vulnerable, convirtiéndo a los usuarios en víctimas potenciales para robarles todo tipo de información de los sistemas de sus víctimas tales como contraseñas o datos personales.

El cliente envía un mensaje HELLO al servidor para solicitar una conexión a través de la suite de cifrado del estándar “RSA”, el atacante mitm modifica este mensaje para solicitar al servidor claves “export RSA”. El servidor responde con una clave RSA de 512 bits firmada con su clave.

El cliente acepta esa clave débil debido a un fallo en OpenSSL/Secure Transport, el atacante Mitm analiza los módulos RSA para recuperar la clave de descifrado RSA correspondiente, cuando el cliente cifra el “pre-master secret” al servidor, el atacante puede ahora descifrarlo para recuperar el “secret master” de TLS.

Desde este momento, el atacante ve en texto plano la comunicación y puede inyectar lo que desee.

3. DETECCIÓN

La prueba consiste en realizar solicitudes a direcciones IPv4 sobre el puerto 443/tcp, intentando establecer una conexión SSL y capturando la respuesta del servidor.

La comprobación se puede realizar en una máquina con Linux usando el siguiente comando:

```
openssl s_client -connect [IP]:443 -cipher EXP-EDH-RSA-DES-CBC-SHA:EXP-EDH-DSS-DESCBC-SHA:EXP-DES-CBC-SHA:EXP-RC2-CBC-MD5:EXP-RC4-MD5
```

También puede verificarlo en la siguiente dirección: https://tools.keycdn.com/freak

INFORMACIÓN DE LOS CAMPOS DEL REPORTE

Campo	Descripción
vulnerabilidad	Nombre de la vulnerabilidad reportada
direccion_ip	Dirección IP del host
puerto	Puerto desde donde se obtiene la respuesta
timestamp_EcuCERT	Fecha y hora de comprobación de EcuCERT en GMT -5
as_name	Nombre del ASN
status_ EcuCERT	**Estado de la vulnerabilidad** **Online:** vulnerabilidad reportada por Feeds y comprobada por el EcuCERT en el timestamp_EcuCERT **Offline:** Vulnerabilidad reportada por Feeds, pero en el timestamp_EcuCERT no se detectó.
timestamp	Fecha y hora de reporte de Shadowserver en UTC+0
ip	Dirección IP del host involucrado
port	Puerto desde donde se obtiene la respuesta SSL
hostname	DNS reverso del host involucrado
tag	Siempre será ssl
handshake	El hadshake de mayor nivel que puede ser negociado (TLSV 1.2, TLS v1.1, TLSv1.0, SSLv3)
asn	ASN donde se encuentra el host involucrado
geo	País donde se encuentra el host involucrado
region	Estado/Provincia/Región donde se encuentra el host involucrado
city	Ciudad donde se encuentra el host
cipher_suite	El cipherSuite más alto que fue capaz de negociar

freak_vulnerable	"Y" indica que el dispositivo permite el uso de cifrado "export-grade" que puede ser usado en un ataque FREAK
freak_chipher_suite	El cifrado "export-grade" con el que se ha realizado la conexión
cert_length	Longitud del certificado (1024 bit, 2048 bit, etc)
subject_common_name	Common Name (CN) del certificado SSL
issuer_common_name	Common Name (CN) de la entidad que ha firmado el certificado SSL
cert_issue_date	Fecha desde la cual es válido el certificado SSL
cert_expiration_date	Fecha en la que expira el certificado SSL

4. ACCIONES RECOMENDADAS

Las medidas que se puede adoptar son las siguientes:

- **Servidores:** Desactivar el soporte para versiones TLS del tipo EXPORT, desactivar SSL y versiones TLS inferiores a la versión 1.2., con esto el atacante no podrá forzar al servidor al uso de algoritmos de cifrado menos seguros.
- **Clientes:** Mantener actualizado los navegadores con la versión más reciente.
- **Administradores y Desarrolladores:** Mantener las librerías TLS actualizadas.

Para deshabilitar el soporte en los servidores Web Apache de Suites de Cifrado del tipo EXPORT es necesario modificar el archivo ssl.conf:

- En Ubuntu el archivo se encuentra en: /etc/apache2/mods-available/ssl.conf
- En Centos el archivo se encuentra en: /etc/httpd/conf.d/ssl.conf

Dentro del archivo encontrar la directiva SSLCipherSuite, y modificarla para remover el soporte de los cifrados tipo EXPORT añadiendo **":: !EXPORT"** al final de esa línea.

Guardar y cerrar el archivo ssl.conf. Reiniciar el servicio para habilitar los cambios:

- En Ubuntu ejecutar: "*service apache2 restart"*
- En Centos ejecutar: "*service httpd restart"*

5. REFERENCIAS

- https://freakscan.shadowserver.org/
- https://www.shadowserver.org/wiki/pmwiki.php/Services/Ssl-Freak-Scan
- https://www.smacktls.com/#freak
- https://wiki.mozilla.org/Security/Server_Side_TLS#Recommended_configurations
- https://tools.keycdn.com/freak

- https://www.ssllabs.com/ssltest/