# Vulnerabilidad débil del modo CBC del protocolo SSLv3 y TLSv1

## Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Requisitos](#)
[Amenaza](#)
[Solución](#)
[Información Relacionada](#)

## Introducción

Este documento describe cómo inhabilitar las cifras del modo del Cipher Block Chaining (CBC) en el dispositivo de seguridad del correo electrónico de Cisco (ESA). Una auditoría de Seguridad/una exploración pudo señalar que un ESA tiene una vulnerabilidad débil del modo CBC del protocolo del v1 de la Seguridad de la capa de Secure Sockets Layer (SSL) v3/Transport (TLS).

## Prerrequisitos

### Requisitos

No hay requisitos específicos para este documento.

### Componentes Utilizados

La información en este documento se basa en AsyncOS para la Seguridad del correo electrónico (cualquier revisión), Cisco ESA, y un ESA virtual.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

# Antecedentes

- La conformidad del estándar PCI DSS (PCI DSS) requiere las cifras CBC ser inhabilitada.
- Una auditoría de Seguridad/una exploración ha identificado una vulnerabilidad potencial con los protocolos del v1 SSL v3/TLS que utilizan las cifras del modo CBC.

  Consejo: El 3.0 del SSL versión (RFC-6101) es un Obsoleto y un protocolo inseguro. Hay una vulnerabilidad en SSLv3 CVE-2014-3566 conocido como Oracle del relleno en el ataque del cifrado de la herencia Downgraded (CANICHE), el Id. de bug Cisco CSCur27131. La recomendación es inhabilitar el v3 SSL mientras que usted cambia las cifras y utiliza TLS solamente, y selecciona el option 3 (v1 de TLS). Revise el Id. de bug Cisco proporcionado CSCur27131 para los detalles completos.

El v3 SSL y los protocolos del v1 de TLS se utilizan para proporcionar la integridad, la autenticidad, y la aislamiento a otros protocolos tales como HTTP y Lightweight Directory Access Protocol (LDAP). Proporcionan estos servicios con el uso del cifrado para la aislamiento, de los Certificados x509 para la autenticidad, y de la funcionalidad de encripción unidireccional para la integridad. Para cifrar los datos, el SSL y TLS pueden utilizar los cifrados en bloque que son los algoritmos de encripción que pueden cifrar solamente un bloque fijo de las informaciones originales a un bloque cifrado del mismo tamaño. Observe que estas cifras obtendrán siempre el mismo bloque resultante para el mismo bloque original de los datos. Para alcanzar la diferencia en la salida, la salida del cifrado es XORed con otro bloque del mismo tamaño designado los vectores de inicialización (iv). El CBC utiliza un IV para el bloque inicial y el resultado del bloque anterior para cada bloque subsiguiente para obtener la diferencia en la salida del cifrado del cifrado en bloque.

En la implementación del v3 SSL y del v1 de TLS, el uso bien escogido del modo CBC era pobre porque el tráfico entero comparte una sesión CBC con un único conjunto de IV iniciales. El resto de los IV está, según lo mencionado previamente, los resultados del cifrado de los bloques anteriores. Los IV subsiguientes están disponibles para los cotillas. Esto permite que un atacante con la capacidad inyecte el tráfico arbitrario en la secuencia del sólo texto (ser cifrado por el cliente) para verificar su conjetura del sólo texto que precede el bloque inyectado. Si la conjetura de los atacantes está correcta, después la salida del cifrado es lo mismo para dos bloques.

Para los datos bajos de la entropía, es posible conjeturar el bloque del sólo texto con relativamente un número bajo de tentativas. Por ejemplo, para los datos que tienen 1000 posibilidades, la cantidad de intentos puede ser 500.

# Requisitos

Hay los varios requerimientos que se deben cumplir para que el exploit trabaje:

1. La conexión SSL/TLS debe utilizar una de las cifras del cifrado del bloque que utilizan al modo CBC, tal como DES o AES.  Los canales que utilizan las cifras de secuencia tales como RC4 no están conforme al defecto. Una proporción grande de conexiones SSL/TLS utiliza el RC4.
2. La vulnerabilidad se puede explotar solamente por alguien que intercepta los datos sobre la conexión SSL/TLS, y también envía activamente los nuevos datos sobre esa conexión. La explotación del defecto hace la conexión SSL/TLS ser terminada. El atacante debe continuar

monitoreando y utilizando las nuevas conexiones hasta que bastantes datos se recopilen para desencriptar el mensaje.
3. Puesto que la conexión se termina cada vez, el cliente SSL/TLS debe poder continuar restableciendo el canal SSL/TLS bastante tiempo para que el mensaje sea desencriptado.
4. La aplicación debe volver a enviar los mismos datos sobre cada conexión SSL/TLS que cree y el módulo de escucha debe poder localizarla en la secuencia de datos. Protocolos como IMAP/SSL que tienen un conjunto fijo de los mensajes para iniciar sesión la reunión este requisito. El web general que hojea no hace.

## Amenaza

La vulnerabilidad CBC es una vulnerabilidad con el v1 de TLS. Esta vulnerabilidad ha estado en la existencia desde principios de 2004, y fue resuelta en versiones posteriores del v1.1 de TLS y del v1.2 de TLS.

Antes de AsyncOS 9.6 para la Seguridad del correo electrónico, el ESA utiliza el v1.0 de TLS y las cifras del modo CBC. Con la versión de AsyncOS 9.6, el ESA introduce el v1.2 de TLS.  No obstante, las cifras del modo CBC pueden ser inhabilitadas, y solamente las cifras RC4 pueden ser utilizadas que no están conforme al defecto.

Además, si se habilita SSLv2 esto puede accionar un falso positivo para esta vulnerabilidad. Es muy importante que el v2 SSL esté inhabilitado.

## Solución

Inhabilite las cifras del modo CBC para dejar solamente las cifras RC4 habilitadas. Fije el dispositivo para utilizar solamente el v1 de TLS, o el v1.2 de TLS v1/TLS:

1. Inicie sesión al CLI.
2. Ingrese el **sslconfig del** comando.
3. Ingrese el comando **GUI**.
4. Elija el número de opción 3 para “TLS el v1", o como se lista en AsyncOS 9.6" TLS v1/TLS el v1.2".
5. Ingrese esta cifra:`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
6. Ingrese el comando: **ENTRANTE**.
7. Elija el número de opción 3 para “TLS el v1", o como se lista en AsyncOS 9.6" TLS v1/TLS el v1.2".
8. Ingrese esta cifra:`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
9. Ingrese el comando outbound.
10. Elija el número de opción 3 para “TLS el v1", o como se lista en AsyncOS 9.6" TLS v1/TLS el v1.2".
11. Ingrese esta cifra:`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
12. Presione ENTER hasta que usted vuelva al prompt del nombre de host.
13. Ingrese el comando commit.
14. Finalize que confía sus cambios.

El ESA ahora se configura para soportar solamente el v1 de TLS, o el v1.2 TLSv1/TLS, con las cifras RC4 mientras que rechaza cualquier filtro CBC.

Aquí está la lista de cifras usadas cuando usted fija RC4:-SSLv2. Observe que no hay cifras del modo CBC en la lista.

```
ECDHE-RSA-RC4-SHA SSLv3 Kx=ECDH Au=RSA Enc=RC4(128) Mac=SHA1
ECDHE-ECDSA-RC4-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=RC4(128) Mac=SHA1
ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
PSK-RC4-SHA SSLv3 Kx=PSK Au=PSK Enc=RC4(128) Mac=SHA1
EXP-ADH-RC4-MD5 SSLv3 Kx=DH(512) Au=None Enc=RC4(40) Mac=MD5 export
EXP-RC4-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
```

Mientras que este exploit es de interés muy bajo debido a su complejidad y requisitos de explotar, el funcionamiento de estos pasos es una gran salvaguardia para la prevención de los exploits posibles, así como pasar las exploraciones estrictas de la Seguridad.

# Información Relacionada

- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems