Desactive los cifrados de modo CBC del servidor SSH en ASA

Contenido

Introducción

Este documento describe cómo inhabilitar los Ciphers en modo CBC del servidor SSH en ASA. En la vulnerabilidad de escaneo CVE-2008-5161 se documenta que el uso de un algoritmo de cifrado de bloques en el modo Cipher Block Chaining (CBC) facilita a los atacantes remotos la recuperación de ciertos datos de texto sin formato de un bloque arbitrario de texto cifrado en una sesión SSH a través de vectores desconocidos.

Cipher Block Chaining (CBC) es un modo de funcionamiento para el bloque cifrado, este algoritmo utiliza un cifrado de bloque para proporcionar un servicio de información como confidencialidad o autenticidad.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Arquitectura de plataforma Adaptive Security Appliance ASA
- Encadenamiento de bloques de cifrado (CBC)

Componentes Utilizados

La información de este documento se basa en un Cisco ASA 5506 con OS 9.6.1.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

De forma predeterminada, en el modo ASA CBC se habilita en el ASA, lo que podría ser una vulnerabilidad para la información de los clientes.

Solución

Después de la mejora CSCum63371, la capacidad de modificar los cifrados ssh ASA se introdujo en la versión 9.1(7), pero la versión que oficialmente tiene los comandos **cifrado ssh cipher** y **integridad ssh cipher** es 9.6.1.

Para inhabilitar los CBC mode Ciphers en SSH, siga este procedimiento:

Ejecute "sh run all ssh" en ASA:

```
ASA(config)# show run all ssh
ssh stricthostkeycheck
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 60
ssh version 2
ssh cipher encryption medium
ssh cipher integrity medium
ssh key-exchange group dh-group1-sha1
```

Si ve el comando **ssh cipher encryption medium**, esto significa que el ASA utiliza cifrados de media y alta potencia que se configura de forma predeterminada en el ASA.

Para ver los algoritmos de cifrado ssh disponibles en el ASA, ejecute el comando **show ssh ciphers**:

```
ASA(config)# show ssh ciphers
Available SSH Encryption and Integrity Algorithms Encryption Algorithms:
       all:     3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr
aes256-ctr
       low:     3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr
aes256-ctr
       medium:  3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr
aes256-ctr
       fips:    aes128-cbc   aes256-cbc
       high:    aes256-cbc   aes256-ctr
Integrity Algorithms:
       all:     hmac-sha1    hmac-sha1-96 hmac-md5     hmac-md5-96
       low:     hmac-sha1    hmac-sha1-96 hmac-md5     hmac-md5-96
       medium:  hmac-sha1    hmac-sha1-96
       fips:    hmac-sha1
       high:    hmac-sha1
```

El resultado muestra todos los algoritmos de cifrado disponibles: **3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr.**

Para inhabilitar el modo CBC para que se pueda utilizar en la configuración ssh, personalice los algoritmos de cifrado que se utilizarán, con el siguiente comando:

```
ssh cipher encryption custom aes128-ctr:aes192-ctr:aes256-ctr
```

Después de esto, ejecute el comando **show run all ssh**, ahora en la configuración de cifrado ssh todos los algoritmos utilizan solamente el modo CTR:

```
ASA(config)# show run all ssh
ssh stricthostkeycheck
```

```
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 60
ssh version 2
ssh cipher encryption custom "aes128-ctr:aes192-ctr:aes256-ctr"
ssh cipher integrity medium
ssh key-exchange group dh-group1-sha1
```

Asimismo, los algoritmos de integridad SSH se pueden modificar con el comando **ssh cipher Integrity**.