Desativar cifras do modo CBC do servidor SSH no ASA

Contents

Introduction

Este documento descreve como desativar os Ciphers do modo CBC do servidor SSH no ASA. Na vulnerabilidade de verificação CVE-2008-5161, está documentado que o uso de um algoritmo de cifra de bloco no modo CBC (Cipher Block Chaining) facilita para os invasores remotos a recuperação de determinados dados de texto simples de um bloco arbitrário de texto cifrado em uma sessão SSH através de vetores desconhecidos.

A CBC (Cipher Block Chaining, cadeia de blocos de cifras) é um modo de operação para o bloco de cifras. Esse algoritmo usa uma cifra de blocos para fornecer um serviço de informação como confidencialidade ou autenticidade.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Adaptive Security Appliance Arquitetura da plataforma ASA
- CBC (Cipher Block Chaining, encadeamento de blocos de cifras)

Componentes Utilizados

As informações neste documento são baseadas em um Cisco ASA 5506 com 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema

Por padrão, o modo ASA CBC está ativado no ASA, o que pode ser uma vulnerabilidade para as informações dos clientes.

Solução

Depois de aprimorar o CSCum63371, a capacidade de modificar as cifras do ASA ssh foi introduzida na versão 9.1(7), mas a versão que oficialmente tem os comandos **ssh cipher encryption** e **ssh cipher Integrity** é 9.6.1.

Para desabilitar o modo CBC Ciphers no SSH, siga este procedimento:

Execute "sh run all ssh" no 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
```

Se você vir o comando **ssh cipher encryption medium**, isso significa que o ASA usa cifras de alta e média intensidade que é configurado por padrão no ASA.

Para ver os algoritmos de criptografia ssh disponíveis no ASA, execute o 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
```

A saída mostra todos os algoritmos de criptografia disponíveis: **3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr.**

Para desabilitar o modo CBC para que ele possa ser usado na configuração ssh, personalize os algoritmos de criptografia a serem usados, com o seguinte comando:

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

Depois disso, execute o comando **show run all ssh**, agora na configuração de criptografia ssh cipher todos os algoritmos usam somente o 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
```

Da mesma forma, os algoritmos de integridade SSH podem ser modificados com o comando **ssh cipher Integrity**.