Disable SSH Server CBC Mode Ciphers on ASA

Contents

Introduction

This document describes how to disable SSH server CBC mode Ciphers on ASA. On scan vulnerability CVE-2008-5161 it is documented that the use of a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plain text data from an arbitrary block of cipher text in an SSH session via unknown vectors.

Cipher Block Chaining (CBC) is a mode of operation for cipher block, this algorithm uses a block cipher to provide an informational service such as confidentiality or authenticity.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Adaptive Security Appliance ASA platform architecture
- Cipher Block Chaining (CBC)

Components Used

The information in this document is based on a Cisco ASA 5506 with 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. If your network is live, ensure that you understand the potential impact of any command.

Problem

By default, on the ASA CBC mode is enabled on the ASA which could be a vulnerability for the customers information.

Solution

After enhancement CSCum63371, the ability to modify the ASA ssh ciphers was introduced on version 9.1(7), but the release that officially has the commands **ssh cipher encryption** and **ssh cipher integrity** is 9.6.1.

In order to disable CBC mode Ciphers on SSH follow this procedure:

Run "sh run all ssh" on the 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
```

If you see the command **ssh cipher encryption medium** this means that the ASA uses medium and high strength ciphers which is setup by default on the ASA.

In order to see the available ssh encryption algorithms in the ASA, run the command **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-c
        low:     3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr   aes256-c
        medium:  3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr   aes256-c
        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
```

The output shows all the available encryption algorithms: **3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr.**

In order to disable CBC mode so it can be used on the ssh configuration, customize the encryption algorithms to be used, with the following command:

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

After this is done, run the command **show run all ssh**, now in the ssh cipher encryption configuration all the algorithms use only CTR mode:

```
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
```

Likewise, the SSH Integrity Algorithms can be modified with the command **ssh cipher integrity**.