Deaktivieren von SSH-Server-CBC-Modus-Ciphers auf ASA

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Ciphers des SSH-Server-CBC-Modus auf ASA deaktiviert werden. Beim Scan-Verwundbarkeit CVE-2008-5161 wird dokumentiert, dass die Verwendung eines Blockchiffrieralgorithmus im Cipher Block Chaining (CBC)-Modus es entfernten Angreifern erleichtert, bestimmte Nur-Text-Daten aus einem beliebigen Codeblock in einer SSH-Sitzung über unbekannte Vektoren wiederherzustellen.

Cipher Block Chaining (CBC) ist ein Betriebsmodus für Verschlüsselungsblöcke. Dieser Algorithmus verwendet eine Blockchiffre, um einen Informationsdienst wie Vertraulichkeit oder Authentizität bereitzustellen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- ASA-Plattformarchitektur der Adaptive Security Appliance
- Cipher Block Chaining (CBC)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einer Cisco ASA 5506 mit OS 9.6.1.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem

Standardmäßig ist der ASA CBC-Modus auf der ASA aktiviert, was eine Schwachstelle für

Kundeninformationen darstellen kann.

Lösung

Nach der Verbesserung CSCum63371 wurde die Möglichkeit eingeführt, die ASA SSH-Verschlüsselungen zu ändern, in Version 9.1(7), aber die Version, die offiziell die Befehle **SSH-Verschlüsselung** und **SSH-Verschlüsselung** hat, ist 9.6.1.

Gehen Sie folgendermaßen vor, um die Ciphers im CBC-Modus auf SSH zu deaktivieren:

Führen Sie "sh run all ssh" auf der ASA aus:

```
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
```

Wenn Sie den Befehl **ssh cipher encryption medium** sehen, bedeutet dies, dass die ASA mittelschwere und hochfeste Chiffren verwendet, die standardmäßig auf der ASA eingerichtet werden.

Um die verfügbaren SSH-Verschlüsselungsalgorithmen in der ASA anzuzeigen, führen Sie den Befehl **show ssh ciphers aus**:

```
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
```

Die Ausgabe zeigt alle verfügbaren Verschlüsselungsalgorithmen an: **3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr.**

Um den CBC-Modus zu deaktivieren, damit er in der SSH-Konfiguration verwendet werden kann, passen Sie die zu verwendenden Verschlüsselungsalgorithmen mit dem folgenden Befehl an:

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

Führen Sie nach diesem Schritt den Befehl **show run all ssh aus**, jetzt in der SSH-Verschlüsselungskonfiguration alle Algorithmen verwenden nur den CTR-Modus:

```
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
```

Ebenso können die SSH Integrity Algorithms mit dem Befehl **ssh cipher integer** geändert werden.