SSH-server CBC-modemkaarten op ASA uitschakelen

Inhoud

Inleiding

Dit document beschrijft hoe u de SSH-server CBC-mode-cifen op ASA kunt uitschakelen. Op scan kwetsbaarheid CVE-2008-5161 is gedocumenteerd dat het gebruik van een algoritme van het blokalgoritme in de modus Cipher Block Chaining (CBC) het voor externe aanvallers gemakkelijker maakt om bepaalde gegevens van onbewerkte tekst uit een willekeurig blok van de tekst in een SSH-sessie te herstellen via onbekende cellen.

Cipher Block Chaining (CBC) is een manier om te werken voor algoritmische blok, dit algoritme gebruikt een blokalgoritme om een informatieve service te geven zoals vertrouwelijkheid of authenticiteit.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Adaptieve security applicatie ASA platform architectuur
- Cipher Block Chaining (CBC)

Gebruikte componenten

De informatie in dit document is gebaseerd op een Cisco ASA 5506 met OS 9.6.1.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Probleem

Standaard is de ASA CBC-modus ingeschakeld op de ASA-methode, wat een kwetsbaarheid voor

de klantinformatie kan zijn.

Oplossing

Na verbetering CSCum63371, werd de mogelijkheid om de ASA ssh-cifen te wijzigen geïntroduceerd op versie 9.1(7), maar de release die officieel de opdrachten heeft met **behulp** van het **ssh-algoritme** en **de integriteit van het ssh-algoritme** is 9.6.1.

Om CBC mode Keiders op SSH uit te schakelen volgt u deze procedure:

Start "sh run all ssh" op de 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
```

Als u het commando **SSH-encryptie medium** ziet, betekent dit dat de ASA middelste en hoge-sterktemakers gebruikt die standaard zijn ingesteld op de ASA.

Om de beschikbare SSH-encryptie-algoritmen in de ASA te zien, **voert** u de opdracht **Sp-ciphers uit**:

```
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
```

De uitvoer toont alle beschikbare encryptie-algoritmen: **3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr.**

Om CBC-modus uit te schakelen, zodat deze op de SSH-configuratie kan worden gebruikt, dient u de te gebruiken encryptie-algoritmen aan te passen, met de volgende opdracht:

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

Nadat dit is gedaan, **voert** de commando **show alle ssh uit**, nu in de ssh encryptie configuratie, alle algoritmen gebruiken slechts 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
```

Op dezelfde manier kan de SSH Integrity Algorithms met de **integriteit** van het **opdrachtalgoritme** worden gewijzigd.