تعطيل عمليات تشفير وضع CBC لخادم SSH على ASA

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
المشكلة
الحل

المقدمة

يصف هذه الوثيقة كيفية تعطيل عمليات تشفير وضع CBC لخادم SSH على ASA. الوثيقة CVE-2008-5161 عند استخدام خوارزمية التشفير في وضع التشفير المتسلسل (CBC) للسماح للمهاجمين البعيدين باسترداد بيانات نص عادي معينة من كتلة التشفير في جلسة SSH عبر متجهات غير معروفة.

وضع التشفير المتسلسل (CBC) هو وضع عملية لكتلة التشفير، تستخدم هذه الخوارزمية تشفير الكتلة لتوفير خدمة إعلامية مثل السرية أو الأصالة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- بنية النظام الأساسي Adaptive Security Appliance ASA
- ربط كتلة التشفير (CBC)

المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى Cisco ASA 5506 مع OS 9.6.1.

تم إنشاء المعلومات الواردة في هذه المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذه المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المشكلة

بشكل افتراضي، يتم تمكين وضع ASA CBC على ASA الذي يمكن أن يكون نقطة ضعف لمعلومات العملاء.

الحل

بعد التحسين CSCum63371، تم إدخال القدرة على تعديل شفرة ASA SSH في الإصدار 9.1(7)، ولكن الإصدار الذي يحتوي رسميا على الأوامر **تشفير SSH** و**تشفير SSH كامل** هو 9.6.1.

لتعطيل شفرات وضع CBC على SSH، اتبع هذا الإجراء:

تشغيل "sh run all ssh" على 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
```

إذا كنت ترى **تشفير SSH متوسط** الأمر، فهذا يعني أن ASA يستخدم شفرة متوسطة وعالية القوة والتي يتم إعدادها بشكل افتراضي على ASA.

لعرض خوارزميات تشفير SSH المتاحة في ASA، قم بتشغيل الأمر **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
```

يعرض الإخراج جميع خوارزميات التشفير المتوفرة: **3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr.**

لتعطيل وضع CBC حتى يمكن إستخدامه على تكوين SSH، قم بتخصيص خوارزميات التشفير التي سيتم إستخدامها، باستخدام الأمر التالي:

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

بعد القيام بذلك، قم بتشغيل الأمر **show run all ssh**، والآن في تكوين تشفير SSH، تستخدم جميع الخوارزميات وضع CTR فقط:

```
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
```

وبالمثل، يمكن تعديل خوارزميات تكامل SSH باستخدام الأمر **ssh cipher integrity**.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).