أستكشاف أخطاء قابلية تشفير CBC وإصلاحها في NCCM 3.8+ و CSPC 2.9+

المحتويات

[المقدمة](#)

[المشكلة](#)

[نهج تقليدي](#)

[الحل](#)

المقدمة

يوضح هذا المستند كيفية أستكشاف أخطاء قابلية تشفير CBC وإصلاحها في NCCM 3.8+ و CSPC 2.9+.

المشكلة

في الإصدارات الأخيرة من CSPC/NCCM، لدينا قابلية ضعيفة لتشفير CBC. في معظم الحالات، يمكنك إصلاحه بتحديث ملفات تكوين SSH المطلوبة. ومع ذلك، تم طرح هذه المقالة لرفض الوصول إليها بشكل صريح من خلال سياسات التشفير. أستخدم هذا إذا فشل لك شيء آخر. لا يمكن أن يؤثر ذلك على سياسات التشفير الافتراضية ولكن بدل من ذلك إضافة طبقة إضافية أعلى النهج الافتراضي.

نهج تقليدي

تأكد من إزالة جميع شفرات CVC من sshD_config. إذا إستمرت المشكلة، يمكنك توفير إدخال فارغ للمعلمة ضمن /etc/sysconfig/sshd.

```
CRYPTO_POLICY=
```

تأكد من أخذ نسخة إحتياطية قبل إجراء أي تعديل.

للتحقق من نجاح هذا الإجراء، قم بتشغيل هذا الأمر على جهازك البعيد:

```
ssh -vv -oCiphers=aes128-cbc,aes256-cbc 127.0.0.1
```

إذا تمت مطالبتك بكلمة مرور أو إضافة مفاتيح RSA، فلا تزال المشكلة قائمة.

الحل

إذا فشل الإجراء السابق، يمكنك إضافة طبقة إضافية من سياسة التشفير عن طريق رفض أي وصول إلى شفرات CBC بشكل صريح. لا يوصى بتغيير أي تكوين افتراضي لنهج التشفير، لذلك ينصح بهذا النهج.

قبل المتابعة، تأكد من عدم وجود طبقات إضافية مطبقة فوق أسلوب التشفير الافتراضي. إذا كانت هناك طبقات إضافية، عندئذ يمكنك مراجعتها قبل عمل أي تغييرات. للتحقق من ذلك، قم بتشغيل هذا الأمر:

```
update-crypto-policies --show
```

الاستجابة هي الافتراضية. إذا كان كذلك، يمكنك المتابعة بالخطوات التالية دون أي تحقق إضافي.

إنشاء ملف جديد تحت المسار المطلق:

```
/etc/crypto-policies/policies/modules/DISABLE-CBC.pmod
```

يمكنك تسمية هذا الملف بأي طريقة لكن الملحق ينتهي بـ .pmod.

بما أننا نزيل هذه الثغرات لتقييد وصول SSH باستخدام هذه المشفرات، فأدخل هذا السطر كإدخال وحيد في هذا الملف الجديد:

```
ssh_cipher = -AES-128-CBC -AES-256-CBC
```

ملاحظة: هذا كمرجع فقط. يمكنك إضافة جميع المشفرات التي تحاول رفضها بشكل صريح، ولكن ينصح بإنشاء ملف جديد لأي تشفير آخر غير CBC لتجنب الارتباك.

بعد حفظ الملف، قم بتعيين قيمة نهج التشفير من الوضع الافتراضي إلى هذه الطبقة الإضافية عن طريق تشغيل هذا الأمر:

```
update-crypto-policies --set DEFAULT:DISABLE-CBC
```

مرة أخرى، يمكن أن تختلف قيمة DISABLE-CBC بناء على الاسم الذي تم توفيره عندما قمت بإنشاء الملف.

يمكنك الآن إعادة التحقق من خلال التشغيل:

```
update-crypto-policies --show
```

هذه المرة، يجب أن تقصير:disable-cbc، مؤكدا أن طبقة إضافي تلقى يكون أضفت دون تعديل التقصير مبرد.

في هذه المرحلة، إذا قمت بإعادة التحقق من الوصول، يتم رفضه:

```
ssh -vv -oCiphers=aes128-cbc,aes256-cbc 127.0.0.1
```

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).