عم Nexus 9000 إلى SSH لوكوتورب نكمي ال أطخلا مالتسإ مت ؛"قباطم ريفشت دجوي ال؛"

المحتويات

المقدمة

يوضح هذا المستند كيفية أستكشاف أخطاء SSH وإصلاحها/حلها إلى Nexus 9000 بعد ترقية الرمز.

الخلفية

قبل شرح أسباب مشاكل SSH، من الضروري معرفة المزيد حول الثغرة في وضع "CBC ل 'SSH Server" التي تم تمكينها وخوارزميات MAC الضعيفة ل SSH التي تم تمكينها' والتي تؤثر على النظام الأساسي Nexus 9000.

معرف CVE - CVE- 2008-5161 (تمكين شفرات وضع SSH CBC وتمكين خوارزميات MAC الضعيفة SSH)

وصف المشكلة - SSH Server CBC Mode Ciphers Enabled Vulnerability (SSH Server CBC Mode Ciphers Enabled)

تم تكوين خادم SSH لدعم تشفير وتصيل كتل التشفير (CBC). قد يسمح ذلك للمهاجم باسترداد رسالة النص العادي من النص المشفر. لاحظ أن هذا الملحق يتحقق فقط من خيارات خادم SSH والوصف الإصدارات البرامج الضعيفة.

حل موصى به - تعطيل تشفير تشفير وضع CBC وتمكين وضع العداد (CTR) أو تشفير وضع العداد (GCM) في Galois/وضع العداد

المرجع - قاعدة البيانات الوطنية للضعف - تفاصيل CVE-2008-5161

المشكلة

بعد ترقية الرمز إلى 7.0(3)I2(1)، يتعذر عليك إدخال SSH في Nexus 9000 واستلام هذا الخطأ:

```
no matching cipher found: client aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc,rijndael-
cbc@lysator.liu.se server
 aes128-ctr,aes192-ctr,aes256-ctr
```

الحل

السبب أنت يعجز أن SSH داخل ال Nexus 9000 بعد أن أنت تقوم بالترقية إلى رمز 7.0(3)I2(1) وفيما بعد ضعيف شفرة معأق عن طريق ال cisco بق id CSCuv39937 إصلاح.

الحل طويل المدى لهذه المشكلة هو إستخدام عميل SSH المحدث/الأحدث الذي يحتوي على شفرة ضعيفة قديمة معطلة.

يمكن الحل المؤقت في إضافة شفرات ضعيفة إلى Nexus 9000. هناك خياران محتملان للحل المؤقت، والذي يعتمد على إصدار الرمز.

خيار مؤقت 1. أمر ضعيف SSH cipher-mode (يتوفر مع NXOS 7.0(3)I4(6) أو أحدث)

- تم تقديمه بواسطة معرف تصحيح الأخطاء من Cisco CSCvc71792 - قم بتنفيذ مقبض للسماح للشفرات الضعيفة aes128-cbc، aes192-cbc، aes256-cbc.
- إضافة دعم لهذه الشفرة الضعيفة - AES128-cbc، AES192-cbc، و AES256-cbc.
- **ال** يوجد حتى الآن **دعم** لشفرة 3des-cbc.

```
! baseline: only strong Ciphers aes128-ctr,aes192-ctr,aes256-ctrallowed
9k# conf t
Enter configuration commands, one per line. End with CNTL/Z.
9k(config)# feature bash
9k(config)# run bash sudo grep -i cipher /isan/etc/dcos_sshd_config
#secure ciphers and MACs
#CSCun41202 : Disable weaker Ciphers and MACs
Ciphers aes128-ctr,aes192-ctr,aes256-ctr    <<-----  only strong ciphers

! enable the weak aes-cbc ciphers with NXOS command
! Note that weak cipher 3des-cbc is still disabled.

9k# conf t
Enter configuration commands, one per line. End with CNTL/Z.
9k(config)# ssh cipher-mode weak
9k(config)# end

!! verification:
9k# run bash sudo grep -i cipher /isan/etc/dcos_sshd_config
#secure ciphers and MACs
#CSCun41202 : Disable weaker Ciphers and MACs
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,aes256-cbc  <<---

! rollback: use the 'no' form of the command
9k# conf t
Enter configuration commands, one per line. End with CNTL/Z.
9k(config)# no ssh cipher-mode weak
9k(config)# end
```

الخيار المؤقت 2. أستخدم base لتعديل ملف ssh_config وإعادة إضافة التشفير الضعيف بشكل صريح

إذا قمت بالتعليق خارج سطر التشفير من ملف /isan/etc/sshd_config، فإن جميع التشفير الافتراضي مدعوم (وهذا يتضمن aes128-cbc، **3des-cbc**، aes192-cbc، و aes256-cbc).

```
n9k#Config t
n9k(config)#feature bash-shell
```

```
n9k(config)#Run bash
bash-4.2$ sudo su -
root@N9K-1#cd /isan/etc
root@N9K-1#cat dcos_sshd_config | egrep Cipher
#CSCun41202 : Disable weaker Ciphers and MACs
Ciphers aes128-ctr,aes192-ctr,aes256-ctr <<<< only allowed ciphers (eliminate known
vulnerability).

!! Create a back up of the existing SSHD_CONFIG
root@N9K-1#mv dcos_sshd_config dcos_sshd_config.backup

!! comment out the cipher line and save to config (effectively removing the restriction)
cat dcos_sshd_config.backup | sed 's@^Cipher@# Cipher@g' > dcos_sshd_config
!! Verify
root@N9K-1#cat dcos_sshd_config | egrep Cipher
#CSCun41202 : Disable weaker Ciphers and MACs
# Ciphers aes128-ctr,aes192-ctr,aes256-ctr << see inserted comment # before Cipher (to remove
the limitation)

root@N9K-1#exit
logout
bash-4.2$ exit
exit
N9K-1(config)# no feature bash
N9K-1(config)# exit
```

لاحظ أنه عند إضافة شفرة قديمة مرة أخرى، تعود إلى إستخدام شفرة ضعيفة، وبالتالي فإنها تعد مخاطرة أمنية.

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).