GetVPN مفاتيح سلوك تغيير

المحتويات

المقدمة

يصف هذا وثيقة ال GETVPN مفتاح تشفير مفتاح (KEK) تغيير سلوك المفتاح. وهو يتضمن الإصدار 15.2(1)T من Cisco IOS® و Cisco IOS-XE 3.5 الإصدار 15.2(1)S). يشرح هذا المستند هذا التغيير في السلوك ومشاكل قابلية التشغيل البيني المحتملة التي يسببها.

تمت المساهمة من قبل وين تشانغ، مهندس TAC من Cisco.

سلوك قديم

قبل cisco ios إطلاق 15.2(1)T، ال kek يرسل مفتاح من قبل المفتاح نادل (KS) عندما ال kek حالي انتهاء. لا يحتفظ عضو المجموعة (GM) بموعد مؤقت لتعقب العمر المتبقي ل KEK. يتم إستبدال KEK الحالي ب KEK جديد فقط عند تلقي مفتاح KEK. إذا لم تحصل الآلية العالمية على مفتاح KEK عند انتهاء صلاحية KEK المتوقع، فإنها لا تؤدي إلى إعادة تسجيل KS، وستبقى KEK الموجود دون السماح بانتهاء صلاحيته. قد يؤدي هذا إلى إستخدام KEK بعد فترة عملها المكونة. أيضا، كتأثير جانبي، لا يوجد أمر على ال GM أن يظهر بقية فترة البقاء ل KEK.

سلوك جديد

يتضمن سلوك مفتاح KEK الجديد تغييرين:

- على KS - يتم إرسال مفاتيح KEK قبل انتهاء صلاحية KEK الحالية، مثل مفتاح تبادل حركة المرور (TEK).
- في GM - تحتفظ GM بموعد لتتبع العمر المتبقي ل KEK وتقوم بإعادة التسجيل في حالة عدم تلقي مفتاح KEK.

سلوك KS الجديد

مع سلوك المفتاح الجديد، يبدأ KS مفتاح KEK قبل انتهاء صلاحية KEK الحالي وفقا لهذه الصيغة.

$$KEK\_rekey\_time = KEK\_lifetime - (200 + (\#\_of\_retran * retran\_interval) + (5 * (1 + \frac{\#\_of\_registered\_GMs}{50})))$$

ملاحظة: في الحساب أعلاه، يتم إستخدام الجزء الأحمر المبرز فقط مع مفتاح إعادة التوجيه للبث الأحادي.

استنادا إلى هذا السلوك، يبدأ KS في إعادة تعيين KEK قبل 200 ثانية على الأقل من انتهاء صلاحية KEK الحالية.
بعد إرسال المفتاح، يبدأ KS في إستخدام ال KEK الجديد لكل مقولات TEK/KEK التالية.

سلوك GM الجديد

يتضمن سلوك جنرال موتورز الجديد تغييرين:

1. إنها تفرض انتهاء صلاحية فترة بقاء KEK بإضافة مؤقت لتتبع فترة بقاء KEK. عندما تنتهي صلاحية المؤقت، يتم حذف KEK في GM ويتم تشغيل إعادة التسجيل.
2. تتوقع GM حدوث مفتاح KEK قبل 200 ثانية على الأقل من انتهاء صلاحية KEK الحالية (راجع تغيير سلوك KS). تتم إضافة مؤقت آخر بحيث في حالة عدم تلقي KEK الجديد قبل انتهاء صلاحية KEK الحالي ب 200 ثانية على الأقل، يتم حذف KEK ويتم تشغيل إعادة التسجيل. يقع حدث حذف KEK وإعادة تسجيله هذا في الفاصل الزمني (انتهاء صلاحية KEK - 190 ثانية، انتهاء صلاحية KEK - 40 ثانية).

وإلى جانب التغييرات الوظيفية، يتم أيضا تعديل مخرجات أمر **عرض** GM لعرض العمر المتبقي ل KEK وفقا لذلك.

```
GM#show crypto gdoi
GROUP INFORMATION

    Group Name : G1
Group Identity : 3333
   Crypto Path : ipv4
Key Management Path : ipv4
  Rekeys received : 0
IPSec SA Direction : Both

Group Server list : 10.1.11.2

Group member : 10.1.13.2 vrf: None
     Version : 1.0.4
Registration status : Registered
Registered with : 10.1.11.2
Reregisters in : 81 sec      <=== Reregistration due to TEK or
                                  KEK, whichever comes first
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 0.0.0.0
Last rekey seq num : 0
Unicast rekey received: 0
Rekey ACKs sent : 0
Rekey Received : never
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 0
After latest register : 0
Rekey Acks sents : 0
```

```
:ACL Downloaded From KS 10.1.11.2
    access-list deny ospf any any
    access-list deny eigrp any any
access-list deny udp any port = 848 any port = 848
    access-list deny icmp any any
    access-list permit ip any any

:KEK POLICY
    Rekey Transport Type : Unicast
Lifetime (secs) : 56     <=== Running timer for remaining KEK
                                lifetime
        Encrypt Algorithm : 3DES
                Key Size : 192
    Sig Hash Algorithm : HMAC_AUTH_SHA
        Sig Key Length (bits) : 1024

:TEK POLICY for the current KS-Policy ACEs Downloaded
:Serial1/0
:IPsec SA
(spi: 0xD835DB99(3627408281
transform: esp-3des esp-sha-hmac
(sa timing:remaining key lifetime (sec): (2228
Anti-Replay(Time Based) : 10 sec interval
```

مشكلات قابلية التشغيل البيني

مع تغيير سلوك إعادة توجيه KEK هذا، يجب مراعاة مشكلة قابلية التشغيل البيني للتعليمات البرمجية عندما قد لا يقوم KS و GM بتشغيل كلا من إصداري IOS اللذين يحملان هذا التغيير.

في حالة تشغيل GM للرمز الأقدم، و KS تقوم بتشغيل الرمز الأحدث، KS يرسل مفتاح KEK قبل انتهاء صلاحية KEK، لكن ليس هناك تأثير عملي آخر ملحوظ. ومع ذلك، إذا قامت الآلية العالمية بتشغيل سجلات الرموز الجديدة مع KS تشغل الرمز الأقدم، فقد تقوم الآلية العالمية بإعادة تسجيل مجالين من مجالات الترجمة الشفوية في المجموعة من أجل تلقي دورة إعادة المفاتيح الرئيسية الجديدة لكل وحدة المفاتيح. تحدث سلسلة من الأحداث عند حدوث ذلك:

1. تقوم GM بإعادة التسجيل قبل انتهاء صلاحية KEK الحالية، نظرا لأن KS ستقوم بإرسال مفتاح KEK فقط عند انتهاء صلاحية KEK الحالي. تتلقى الآلية العالمية ال KEK، وهي نفس ال KEK التي لديها حاليا مع أقل من 190 ثانية مدى الحياة المتبقية. وهذا يخبر الصحيفة انه مسجل مع KS دون تغيير مفتاح KEK.

```
GDOI-4-GM_RE_REGISTER: The IPSec SA created for group G1 may%
have expired/been cleared, or didn't go through. Re-register to KS. %CRYPTO-5-GM_REGSTER:
                                Start registration to KS 10.1.11.2 for
group G1 using address 10.1.13.2 %GDOI-5-GM_REKEY_TRANS_2_UNI: Group G1 transitioned to
Unicast Rekey. %GDOI-5-SA_KEK_UPDATED: SA KEK was updated %GDOI-5-SA_TEK_UPDATED: SA TEK
was updated %GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.11.2 complete
for group G1 using address 10.1.13.2 %GDOI-5-GM_INSTALL_POLICIES_SUCCESS: SUCCESS:
                                Installation of
Reg/Rekey policies from KS 10.1.11.2 for group G1 & gm identity 10.1.13.2
```

2. يحذف GM KEK عند انتهاء صلاحية حياته، ويضبط مؤقت إعادة التسجيل (انتهاء صلاحية KEK، انتهاء صلاحية KEK + 80).

```
GDOI-5-GM_DELETE_EXPIRED_KEK: KEK expired for group G1 and was deleted%
```

3. عند انتهاء صلاحية مؤقت إعادة التسجيل، تقوم GM بإعادة التسجيل وستتلقى KEK الجديد.

```
GDOI-4-GM_RE_REGISTER: The IPSec SA created for group G1 may%
.have expired/been cleared, or didn't go through. Re-register to KS
CRYPTO-5-GM_REGSTER: Start registration to KS 10.1.11.2 for%
group G1 using address 10.1.13.2 %GDOI-5-GM_REKEY_TRANS_2_UNI: Group G1 transitioned to
Unicast Rekey. %GDOI-5-SA_KEK_UPDATED: SA KEK was updated %GDOI-5-SA_TEK_UPDATED: SA TEK
was updated %GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.11.2 complete for
group G1 using address 10.1.13.2 %GDOI-5-GM_INSTALL_POLICIES_SUCCESS: SUCCESS: Installation
of
Reg/Rekey policies from KS 10.1.11.2 for group G1 & gm identity
10.1.13.2
```

التوصيات

في نشر GETVPN، إذا تمت ترقية أي من رموز GM Cisco IOS إلى أحد الإصدارات باستخدام سلوك مفتاح KEK الجديد، توصي Cisco بترقية رمز KS أيضا لتجنب مشكلة قابلية التشغيل البيني.

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).