КЛЮЧЕВЫЕ GETVPN повторно вводят изменение поведения

Содержание

Введение

Этот документ описывает Ключ шифрования (KEK) GETVPN, повторно вводят изменения поведения. Это включает Cisco IOS® Release 15.2 (1) T) и Cisco IOS XE 3.5 Выпуска 15.2 (1) S). Этот документ объясняет это изменение в поведении и потенциальных проблемах совместимости, вызванных им.

Внесенный Вэнь Чжаном, специалистом службы технической поддержки Cisco.

Старое поведение

До Cisco IOS Release 15.2 (1) T, KEK повторно вводит, передается Сервером ключей (KS), когда истекает текущий KEK. Элемент группы (GM) не поддерживает таймер для отслеживания оставшийся срок действия KEK. Текущий KEK заменен новым KEK только, когда KEK повторно вводит, получен. Если GM не получает KEK, повторно вводят при ожидаемом истечении KEK, это не инициирует перерегистрацию к KS, и это поддержит существующий KEK, не позволяя ему истечь. Это могло привести к KEK, используемому после его настроенного срока действия. Кроме того, как побочный эффект, нет никакой команды на GM, который показывает остающееся время жизни KEK.

Новое поведение

Новый KEK повторно вводит поведение, включает два изменения:

- На KS - KEK повторно вводит, передаются перед истечением текущего ключа, во многом как Ключ обмена трафиком (TEK) повторно вводят.
- На GM - GM поддерживает таймер для отслеживания остающееся время жизни KEK и

инициирует перерегистрацию, если KEK повторно вводит, не получен.

KS новое поведение

С новым повторно вводят поведение, KS запускается, KEK повторно вводят перед истечением текущего ключа согласно этой формуле.

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

Примечание: В вышеупомянутом вычислении красная выделенная часть только используется с индивидуальной рассылкой, повторно вводят.

На основе этого поведения KS начинает повторно вводить KEK по крайней мере за 200 секунд до того, как истечет текущий KEK. После того, как повторно введение передается, KS начинает использовать новый KEK для всего последующего TEK/KEK, повторно вводит.

GM новое поведение

Новое поведение GM включает два изменения:

1. Это принуждает истечение времени жизни KEK путем добавления таймера для отслеживания оставшийся срок действия KEK. Когда тот таймер истекает, KEK удален на GM, и перерегистрация инициирована.
2. GM ожидает, что KEK повторно вводит для появления по крайней мере 200 секунд до истечение текущего ключа (см., что поведение KS изменяется). Другой таймер добавлен так, чтобы в конечном счете новый KEK не был получен по крайней мере за 200 секунд до истечения текущего ключа удален KEK, и перерегистрация инициирована. Этот случай удаления и перерегистрации KEK происходит в интервале таймера (истечение KEK - 190 секунд, истечение KEK - 40 секунд).

Наряду с функциональными изменениями, **выходные данные команды show** GM также модифицируются для отображения оставшегося срока действия KEK соответственно.

```
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
```

Проблемы совместимости

С этим KEK повторно вводят изменение поведения, проблему совместимости кода нужно рассмотреть, когда KS и GM не могли бы выполнить обе из версий IOS, которые имеют это изменение.

В случае, куда GM выполняет более старый код, и KS выполняет более новый код, KS отсылает KEK, повторно вводят до истечения KEK, но нет никакого другого известного функционального влияния. Однако, если GM, выполняющий более новые кодовые регистры с KS выполнение более старого кода, GM может подвергнуться двум перерегистрации Домена группы интерпретации (GDOI) для получения нового KEK на KEK, повторно вводят цикл. Последовательность событий происходит, когда это происходит:

1. GM повторно регистрирует перед истечением текущего ключа, так как KS только передаст KEK, повторно вводят, когда истекает текущий KEK. GM получает KEK, и это - тот же KEK как тот, который это в настоящее время имеет меньше остающийся срок действия 190 секунд. Это говорит GM, что зарегистрировано в KS без KEK, повторно

вводят изменение.

```
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
```

2. GM удаляет KEK при его пожизненном истечении и устанавливает перерегистрационный таймер (истечение KEK, истечение KEK + 80).

```
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
```

3. Когда перерегистрационный таймер истекает, GM повторно регистрирует и получит новый KEK.

```
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
```

Рекомендации

В развертываниях GETVPN, если какой-либо Код Cisco IOS GM был обновлен к одной из версий с новым KEK, повторно вводят поведение, Cisco рекомендует, чтобы код KS был обновлен также для предотвращения проблемы совместимости.