Modifica comportamento reimpostazione chiave GETVPN

Sommario

[Introduzione](#)
[Comportamento precedente](#)
[Nuovo comportamento](#)
[Nuovo comportamento KS](#)
[Comportamento nuovo GM](#)
[Problemi di interoperabilità](#)
[Raccomandazioni](#)

Introduzione

In questo documento vengono descritte le modifiche al comportamento della chiave di crittografia GETVPN (KEK). Include Cisco IOS® versione 15.2(1)T) e Cisco IOS-XE 3.5 versione 15.2(1)S). Questo documento spiega i cambiamenti di comportamento e i potenziali problemi di interoperabilità causati.

Contributo di Wen Zhang, Cisco TAC Engineer.

Comportamento precedente

Nelle versioni precedenti a Cisco IOS versione 15.2(1)T, la chiave viene inviata dal server chiavi (KS) quando scade la chiave corrente. Il membro del gruppo (GM) non gestisce un timer per tenere traccia della durata residua del KEK. La chiave KEK corrente viene sostituita da una nuova chiave KEK solo quando si riceve una nuova chiave KEK. Se il GM non riceve una nuova chiave KEK alla scadenza prevista del KEK, non attiva una nuova registrazione nel KS e manterrà la chiave esistente senza lasciarla scadere. Ciò potrebbe determinare l'utilizzo del KEK dopo la sua durata configurata. Inoltre, come effetto collaterale, non esiste alcun comando sull'oggetto GM che mostri la durata residua del KEK.

Nuovo comportamento

Il nuovo comportamento della chiave KEK include due modifiche:

- In KS - KEK le chiavi vengono inviate prima della scadenza dell'attuale chiave KEK, in modo simile a una chiave di scambio traffico (TEK).
- Sul GM - Il GM mantiene un timer per tenere traccia della durata restante del KEK e attiva una

nuova registrazione se non viene ricevuta la chiave KEK.

Nuovo comportamento KS

Con il nuovo comportamento di reimpostazione delle chiavi, il KS avvia una reimpostazione delle chiavi KEK prima della scadenza corrente in base a questa formula.

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

Nota: Nel calcolo sopra riportato, la parte evidenziata in rosso viene utilizzata solo con una nuova chiave unicast.

In base a questo comportamento, un KS inizia a reimpostare la chiave di un KEK almeno 200 secondi prima della scadenza del KEK corrente. Dopo l'invio della nuova chiave, il KS inizia a utilizzare la nuova chiave per tutte le successive richiavi TEK/KEK.

Comportamento nuovo GM

Il nuovo comportamento GM comprende due modifiche:

1. Impone la scadenza di una durata KEK aggiungendo un timer per tenere traccia della durata restante KEK. Alla scadenza del timer, il KEK viene eliminato dal GM e viene attivata una nuova registrazione.
2. Il GM prevede che la rigenerazione della chiave KEK avvenga almeno 200 secondi prima della scadenza corrente della chiave (vedere Modifica del comportamento KS). Viene aggiunto un altro timer in modo che, nel caso in cui la nuova chiave KEK non venga ricevuta almeno 200 secondi prima della scadenza della chiave corrente, la chiave KEK viene eliminata e viene attivata una nuova registrazione. Questo evento di eliminazione e registrazione KEK si verifica nell'intervallo del timer di (scadenza KEK - 190 secondi, scadenza KEK - 40 secondi).

Oltre alle modifiche funzionali, vengono modificati anche gli output del comando **show** GM per visualizzare la durata rimanente del 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
```

Problemi di interoperabilità

Con questa modifica del comportamento di reimpostazione delle chiavi KEK, è necessario considerare il problema di interoperabilità del codice quando KS e GM potrebbero non eseguire entrambe le versioni IOS che hanno questa modifica.

Nel caso in cui il GM esegua il codice precedente e il KS esegua quello più recente, il KS invia la chiave di rigenerazione KEK prima della scadenza del KEK, ma non vi sono altri impatti funzionali degni di nota. Tuttavia, se un GM che esegue il codice più recente si registra con un KS che esegue il codice meno recente, il GM potrebbe subire due registrazioni GDOI (Group Domain of Interpretation) per ricevere la nuova chiave KEK per ciclo di rigenerazione chiavi KEK. Una sequenza di eventi si verifica quando:

1. Il GM si registra nuovamente prima della scadenza del KEK corrente, poiché il KS invierà la

nuova chiave KEK solo alla scadenza del KEK corrente. Il GM riceve il KEK, ed è lo stesso KEK che ha attualmente con meno di 190 secondi di durata rimanenti. Ciò indica all'GM che è registrato con un KS senza la modifica della chiave del 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. Il GM elimina il KEK alla scadenza della sua durata e imposta un timer di registrazione di (scadenza KEK, scadenza KEK + 80).

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

3. Alla scadenza del timer di registrazione, GM si registra nuovamente e riceve il nuovo 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
```

Raccomandazioni

In un'implementazione GETVPN, se uno dei codici Cisco IOS GM è stato aggiornato a una delle versioni con il nuovo comportamento di reimpostazione delle chiavi KEK, Cisco consiglia di aggiornare anche il codice KS per evitare il problema di interoperabilità.