Identificazione e mitigazione dello sfruttamento della vulnerabilità del decapsulamento GRE

Identificazione e mitigazione dello sfruttamento della vulnerabilità del decapsulamento GRE

ID advisory: cisco-amb-20060912-gre

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20060912-gre

Revisione 1.0

Per la versione pubblica 2006 settembre 12 17:00 UTC (GMT)

Sommario

Risposta di Cisco

Caratteristiche di vulnerabilità

La vulnerabilità della decapsulazione del GRE di Cisco IOS può essere sfruttata in remoto senza autenticazione e senza necessità di interazione da parte dell'utente. Se utilizzato, l'utente malintenzionato potrebbe causare l'inoltro da parte del software Cisco IOS? di pacchetti IPv4 creati appositamente che potrebbero essere utilizzati per ignorare gli elenchi di controllo di accesso. Il vettore di attacco utilizza il protocollo IP 47, Generic Routing Encapsulation (GRE). Questa vulnerabilità non è coperta da un ID CVE.

Questo documento contiene informazioni per aiutare i clienti Cisco a mitigare i tentativi di sfruttare la vulnerabilità della decapsulazione del GRE di Cisco IOS. Questa vulnerabilità influisce sui dispositivi che eseguono il software Cisco IOS configurato con i tunnel GRE. Come definito in origine nella RFC1701, il campo Intestazione GRE contiene un numero di bit di flag deprecati da RFC2784. Questa vulnerabilità non interessa le versioni del software Cisco IOS che supportano RFC2784.

Le informazioni sul software vulnerabile, non interessato e fisso sono disponibili nella risposta di sicurezza PSIRT:

Cisco Security Risposta a: Vulnerabilità del decapsulamento GRE di Cisco IOS

Panoramica delle tecniche di mitigazione

I dispositivi Cisco forniscono diverse contromisure per la vulnerabilità della decapsulazione del GRE di Cisco IOS. La protezione del tunnel sotto forma di incapsulamento IPSec è il mezzo più efficace per ridurre gli attacchi. Per ridurre questo attacco, è possibile anche applicare un elenco degli accessi nella direzione in entrata del traffico GRE e filtrare il protocollo GRE da tutti gli indirizzi di origine ad eccezione di quelli attendibili. Si noti che un attacco può comunque avere esito positivo se il pacchetto GRE viene falsificato utilizzando un indirizzo IP di origine attendibile autorizzato dall'elenco degli accessi applicato.

Gestione dei rischi

Si consiglia alle organizzazioni di seguire i processi standard di valutazione e mitigazione dei rischi per determinare l'impatto potenziale di [questa vulnerabilità|queste vulnerabilità]. Triage si riferisce all'ordinamento dei progetti e all'assegnazione delle priorità agli sforzi che hanno maggiori probabilità di avere successo. Cisco ha fornito documenti che possono aiutare le organizzazioni a sviluppare una funzionalità di triage basata sui rischi per i team addetti alla sicurezza delle informazioni. Valutazione dei rischi per la vulnerabilità della sicurezza Gli annunci e la valutazione dei rischi e la creazione di prototipi possono aiutare le organizzazioni a sviluppare processi ripetibili di valutazione della sicurezza e di risposta.

Mitigazione e identificazione specifiche del dispositivo

Per questi dispositivi sono disponibili informazioni specifiche su mitigazione e identificazione

- Router per edge Internet e terminazione GRE
- Router VPN
- Cisco ASA e PIX Firewall
- NetFlow

Router per edge Internet e terminazione GRE

Attenzione: l'efficacia di qualsiasi tecnica di mitigazione dipende dalle situazioni specifiche del cliente, come il mix di prodotti, la topologia di rete, il comportamento del traffico e la missione organizzativa. Come per qualsiasi modifica apportata alla configurazione, valutare l'impatto della configurazione prima di applicare la modifica.

Attenuazione: elenco accessi interfaccia

Il seguente elenco degli accessi consente l'uso del protocollo IP numero 47 (GRE) su pacchetti provenienti da un singolo host noto (ad esempio, 192.0.2.1) e destinati al router IOS (ad esempio, 192.0.2.2). Tutti gli altri pacchetti GRE sono filtrati.

Le voci aggiunte agli elenchi degli accessi devono essere implementate come parte di un elenco di controllo degli accessi di transito che filtra il traffico di transito e di confine ai punti di ingresso

della rete.

Per ulteriori informazioni sugli ACL, consultare il documento Access Control List transit: Filtering at Your Edge.

```
!-- Allow the GRE protocol from trusted source addresses only. !-- Block GRE from all other source addresses. access-list 100 permit gre host 192.0.2.1 host 192.0.2.2
access-list 100 deny gre any any !-- Permit all other traffic not specifically blocked. access-list 100 permit ip any any !-- Apply access list to interface in the inbound direction. interface Ethernet 0/0 ip access-group 100 in
```

Attenuazione: anti-spoofing

Questa vulnerabilità può essere sfruttata da un pacchetto oggetto di spoofing. La protezione anti-spoof sotto forma di inoltro di percorso inverso unicast può fornire una riduzione limitata se configurata correttamente. Questa funzione non deve essere utilizzata per fornire una riduzione del 100% in quanto i pacchetti oggetto di spoofing possono ancora entrare nella rete dall'interfaccia prevista da uRPF o consentita dagli elenchi degli accessi anti-spoofing. Inoltre, occorre fare in modo che la modalità uRPF appropriata (libera o rigida) sia configurata in modo da garantire che i pacchetti legittimi non vengano scartati.

Ulteriori informazioni sull'inoltro inverso dei percorsi unicast sono disponibili all'indirizzo http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ft_urpf.html.

Attenuazione: ID tunnel GRE

L'applicazione di una chiave ID del tunnel può contribuire a risolvere questo problema, ma il comando non è inteso come funzionalità di sicurezza e la chiave può essere trovata sniffando pacchetti GRE legittimi. Per ulteriori informazioni su questa funzione, consultare il documento sulla configurazione delle interfacce logiche - configurazione della chiave di identificazione del tunnel.

Sul Supervisor 720, i tunnel GRE che usano una chiave ID vengono elaborati in un software che può influire sulle prestazioni.

Identificazione

Dopo aver applicato l'elenco degli accessi all'interfaccia in entrata del GRE, il comando **show access-list <*numero acl*>**può essere usato per identificare il numero di pacchetti da filtrare. I pacchetti filtrati devono essere esaminati per determinare se sono tentativi di sfruttare questo problema. Di seguito è riportato l'output di esempio per **show access-list 100**:

```
Edge-Router#show access-list 100
Extended IP access list 100
10 permit gre host 192.0.2.1 host 192.0.2.2 (141 matches)
20 deny gre any any (100 matches)
30 permit ip any any
```

Nell'esempio precedente, 100 pacchetti GRE sono stati scartati dall'elenco degli accessi configurato in entrata sull'interfaccia Ethernet 0/0.

Router VPN

Attenzione: l'efficacia di qualsiasi tecnica di mitigazione dipende dalle situazioni specifiche del cliente, come il mix di prodotti, la topologia di rete, il comportamento del traffico e la missione organizzativa. Come per qualsiasi modifica apportata alla configurazione, valutare l'impatto della configurazione prima di applicare la modifica.

Attenuazione: GRE protetto da IPSec

La crittografia dei tunnel GRE con IPSec è il mezzo più efficace per prevenire gli attacchi. Per ulteriori informazioni sulla crittografia del GRE con IPSec, fare riferimento alle seguenti risorse:

- Configurazione di un tunnel GRE su IPSec con OSPF
- Configurazione di IPSec/GRE con NAT
- Esempio di configurazione di GRE over IPSec con EIGRP per il routing tramite un hub e più siti remoti
- Configurazione di IPSec (chiavi precondivise) da router a router sul tunnel GRE con CBAC e NAT

Attenuazione: elenco accessi interfaccia

Il seguente elenco degli accessi filtra il protocollo IP numero 47 (GRE) da tutti gli host. I router VPN che terminano il GRE incapsulato in IPSec non devono ricevere pacchetti GRE non crittografati sull'interfaccia in entrata fisica.

Le voci aggiunte agli elenchi degli accessi devono essere implementate come parte di un elenco di controllo degli accessi di transito che filtra il traffico di transito e di confine ai punti di ingresso della rete.

Per ulteriori informazioni sugli ACL, consultare il documento Access Control List transit: Filtering at Your Edge.

Il seguente elenco degli accessi consente il traffico IPSec proveniente da un singolo host trusted (ad esempio, 192.0.2.1) e destinato al router di terminazione IPSec (ad esempio, 192.0.2.2).

```
!-- Block all GRE to the IPSec terminating physical interface. access-list 100 deny
gre any any !-- Permit ESP (IP protocol 50) and !-- ISAKMP UDP ports 500 and 4500.
access-list 100 permit esp host 192.0.2.1 host 192.0.2.2 access-list 100 permit udp
host 192.0.2.1 host 192.0.2.2 eq 500 access-list 100 permit udp host 192.0.2.1 host
192.0.2.2 eq 4500 !-- Permit all other traffic. access-list 100 permit ip any any !--
Apply access list to interface in the inbound direction. interface Ethernet 0/0 ip
access-group 100 in
```

Per l'elenco degli accessi all'interfaccia potrebbe essere necessaria una voce specifica nell'elenco degli accessi per i pacchetti GRE dall'indirizzo IP di origine del tunnel GRE all'indirizzo IP di destinazione del tunnel GRE, se la versione IOS in esecuzione sul dispositivo non dispone della correzione per l'ID bug Cisco CSCdu58486 (solo utenti registrati).

Attenuazione: ID tunnel GRE

L'applicazione di una chiave ID del tunnel può contribuire a risolvere questo problema, ma il

comando non è inteso come funzionalità di sicurezza e la chiave può essere trovata sniffando pacchetti GRE legittimi. Per ulteriori informazioni su questa funzione, consultare il documento sulla configurazione delle interfacce logiche - configurazione della chiave di identificazione del tunnel.

Identificazione

Dopo aver applicato l'elenco degli accessi in transito all'interfaccia fisica in entrata, il comando **show access-list <*numero acl*>** può essere usato per identificare il numero di pacchetti da filtrare. I pacchetti filtrati devono essere esaminati per determinare se sono tentativi di sfruttare questa vulnerabilità. Di seguito è riportato l'output di esempio per **show access-list 100**:

```
Edge-Router#show access-list 100
Extended IP access list 100
10 deny gre any any (100 matches)
20 permit esp host 192.0.2.1 host 192.0.2.2
30 permit udp host 192.0.2.1 host 192.0.2.2 eq 500
40 permit udp host 192.0.2.1 host 192.0.2.2 eq 4500
50 permit ip any any
```

Nell'esempio precedente, 100 pacchetti GRE sono stati scartati dall'elenco degli accessi configurato in entrata sull'interfaccia Ethernet 0/0.

Cisco ASA e PIX Firewall

Attenzione: l'efficacia di qualsiasi tecnica di mitigazione dipende dalle situazioni specifiche del cliente, come il mix di prodotti, la topologia di rete, il comportamento del traffico e la missione organizzativa. Come per qualsiasi modifica apportata alla configurazione, valutare l'impatto della configurazione prima di applicare la modifica.

Attenuazione

I seguenti elenchi degli accessi permettono di usare il protocollo IP numero 47 (GRE) per i pacchetti da un singolo host trusted (ad esempio, 192.0.2.1) e destinati al router IOS con terminazione GRE (ad esempio, 192.0.2.1) 192.0.2.2). Tutti gli altri pacchetti GRE sono filtrati.

PIX 6.x

```
!-- Allow the GRE protocol from trusted source addresses only. !-- Block GRE from all other source addresses. access-list block-gre permit gre host 192.0.2.1 host 192.0.2.2 access-list block-gre deny gre any any !-- Permit/deny all other traffic in accordance with existing security !-- policies and configurations. !-- Apply access list to interface inbound. access-group block-gre in interface outside
```

PIX/ASA 7.x

Come dispositivo di transito, consenti solo agli indirizzi IP di origine attendibili di inviare i pacchetti GRE ai dispositivi all'interno del firewall.

```
!-- Allow the GRE protocol from trusted source addresses only. !-- Block GRE from all
```

```
other source addresses. access-list block-gre extended permit gre host 192.0.2.1 host
192.0.2.2 access-list block-gre extended deny gre any any !-- Permit/deny all other
traffic in accordance with existing security !-- policies and configurations. !--
Apply access list to interface in the inbound direction. access-list block-gre
extended permit ip any any access-group block-gre in interface outside
```

Identificazione

PIX 6.x

Nell'esempio, sono stati ricevuti e bloccati 100 pacchetti GRE.

```
pix#show access-list block-gre
access-list block-gre; 2 elements
access-list block-gre line 1 permit gre host 192.0.2.1 host 192.0.2.2 (hitcnt=0)
access-list block-gre line 2 deny gre any (hitcnt=100)
```

PIX/ASA 7.x

Nell'esempio, sono stati ricevuti e bloccati 100 pacchetti GRE.

```
asa#show access-list block-gre
access-list block-gre; 2 elements
access-list block-gre line 1 extended permit gre host 192.0.2.1 host 192.0.2.2
(hitcnt=50)
access-list block-gre line 2 extended deny gre any (hitcnt=100)
```

In PIX/ASA 7.x, se il GRE è autorizzato attraverso il firewall, usare il comando **show conn | include GRE** può essere utilizzato per verificare le connessioni GRE specifiche in transito attraverso il firewall. È necessario esaminare le connessioni GRE stabilite in modo imprevisto per determinare se si tratta di tentativi di sfruttare il problema. Di seguito è riportato un esempio di output per **show conn | includere GRE**:

```
asa#show conn | include GRE
GRE out 192.0.2.1:0 in 192.0.2.2:0 idle 0:00:15 bytes 3120 flags
GRE out 192.0.2.1:0 in 192.0.2.2:0 idle 0:00:15 bytes 2600 flags
```

NetFlow

Èpossibile configurare NetFlow sui router di perimetro Internet e di terminazione GRE per determinare se sono in corso tentativi di sfruttare questa vulnerabilità.

```
router#show ip cache flow

IP packet size distribution (15014 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  1 active, 65535 inactive, 2 added
```

```
  30 lager polls, 0 flow al loc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402120 bytes
  0 active, 16384 inactive, 0 added, 0 added to flow
  0 al loc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pt     /Sec     /Flow     /Flow
TCP-WWW              2      0.0         1    60      0.0       0.0      15.5
TCP-other            4      0.0         1    60      0.0       0.0      15.7
UDP-other            4      0.0         2   162      0.0       2.7      15.6
ICMP                11      0.0         4    85      0.0       3.0      15.7
GRE               2015     50.0       100   124      0.3       8.7      15.6
IP-other             1      0.0        34   136      0.0      33.3      15.6
Total:            2037     50.0         4   124      0.3       1.3      15.6

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0         192.168.0.1     Fa2/0         192.168.0.2     2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.3     2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.4     2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.5     2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.6     2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.7     2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.8     2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.9     2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.10    2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.11    2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.12    2F 0000 0000   100
---------- Output Truncated ----------
```

Nell'esempio precedente, è presente un numero molto elevato di flussi GRE (Protocol Hex 2F) da un singolo indirizzo IP a più indirizzi IP di destinazione. Sui router perimetrali Internet e potenzialmente sui router di terminazione GRE, ciò può indicare un tentativo di sfruttare questa vulnerabilità e deve essere confrontato con l'utilizzo di base di queste porte sui dispositivi di monitoraggio.

Per visualizzare solo i flussi GRE (Protocol Hex 2F), usare il comando **show ip cache flow | inc SrcIf|2F** può essere utilizzato come indicato di seguito:

```
Router#show ip cache flow | inc SrcIf|2F
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0         192.168.0.1     Fa2/0         192.168.0.2     2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.3     2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.4     2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.5     2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.6     2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.7     2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.8     2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.9     2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.10    2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.11    2F 0000 0000   100
Fa0/0         192.168.0.1     Fa2/0         192.168.0.12    2F 0000 0000   100
---------- Output Truncated ----------
```

Ulteriori informazioni

PER UNO SCOPO SPECIFICO. L'UTILIZZO DA PARTE DELL'UTENTE DELLE INFORMAZIONI CONTENUTE NEL DOCUMENTO O NEI MATERIALI ACCESSIBILI DAL DOCUMENTO AVVIENE A PROPRIO RISCHIO. CISCO SI RISERVA IL DIRITTO DI MODIFICARE O AGGIORNARE IL PRESENTE DOCUMENTO IN QUALSIASI MOMENTO.

Cronologia delle revisioni

Revisione 1.0	12 settembre 2006	Pubblicazione iniziale.

Procedure di sicurezza di Cisco

Le informazioni complete sulla segnalazione delle vulnerabilità della sicurezza nei prodotti Cisco, su come ottenere assistenza in caso di incidenti relativi alla sicurezza e su come registrarsi per ricevere informazioni sulla sicurezza da Cisco, sono disponibili sul sito Web di Cisco all'indirizzo https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html. Ciò include istruzioni per le richieste della stampa relative agli avvisi di sicurezza Cisco. Tutti gli avvisi sulla sicurezza Cisco sono disponibili all'indirizzo http://www.cisco.com/go/psirt.

Informazioni correlate

- Miglioramento della sicurezza sui router Cisco - Protezione del routing IP
- RFC 2827: Filtro ingresso di rete: eliminazione degli attacchi Denial of Service che utilizzano lo spoofing degli indirizzi di origine IP
- Modalità Loose di inoltro percorso inverso unicast
- Configurazione di IPSec Network Security
- Configurazione di un tunnel GRE su IPSec con OSPF
- Configurazione di IPSec/GRE con NAT
- Esempio di configurazione di GRE over IPSec con EIGRP per il routing tramite un hub e più siti remoti
- Configurazione di IPSec (chiavi precondivise) da router a router sul tunnel GRE con CBAC e NAT

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).