Identifizieren und Eindämmen der Ausnutzung der GRE-Entkapselungsschwachstelle

Identifizieren und Eindämmen der Ausnutzung der GRE-Entkapselungsschwachstelle

Beratungs-ID: cisco-amb-20060912-gre

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

Version 1.0

Zur öffentlichen Veröffentlichung 2006 12. September 17:00 UTC (GMT)

Inhalt

Antwort von Cisco

Merkmale der Schwachstelle

Die Cisco IOS GRE-Entkapselungsschwachstelle kann per Remote-Zugriff ohne Authentifizierung und ohne Benutzerinteraktion ausgenutzt werden. Wird dieser ausgenutzt, kann der Angreifer die Cisco IOS?-Software dazu veranlassen, speziell erstellte IPv4-Pakete weiterzuleiten, die möglicherweise verwendet werden könnten, um Zugriffskontrolllisten zu umgehen. Der Angriffsvektor wird über das IP-Protokoll 47, Generic Routing Encapsulation (GRE), abgewickelt. Diese Schwachstelle wird nicht durch eine CVE-ID abgedeckt.

Dieses Dokument enthält Informationen, die Cisco Kunden helfen sollen, Versuche zur Ausnutzung der Cisco IOS GRE-Entkapselungsschwachstelle zu vermeiden. Diese Schwachstelle betrifft Geräte, auf denen Cisco IOS-Software ausgeführt wird und die mit GRE-Tunneln konfiguriert sind. Wie ursprünglich in RFC1701 definiert, enthält das GRE-Header-Feld eine Anzahl von Flagbits, die durch RFC2784 veraltet wurden. Versionen der Cisco IOS-Software, die RFC2784 unterstützen, sind von dieser Sicherheitslücke nicht betroffen.

Anfällige, nicht betroffene und feste Software-Informationen sind in der PSIRT Security Response verfügbar:

Cisco Security Antwort auf: Cisco IOS GRE-Entkapselungsschwachstelle

Überblick über die Risikominderungstechnik

Cisco Geräte bieten verschiedene Gegenmaßnahmen für die Cisco IOS GRE-Entkapselungsschwachstelle. Der Tunnelschutz in Form der IPSec-Kapselung ist das effektivste Mittel zur Eindämmung von Angriffen. Dieser Angriff kann auch dadurch abgewehrt werden, dass eine Zugriffsliste in Richtung des eingehenden GRE-Datenverkehrs angewendet wird und das GRE-Protokoll von allen außer vertrauenswürdigen Quelladressen gefiltert wird. Beachten Sie, dass ein Angriff immer noch erfolgreich sein kann, wenn das GRE-Paket mithilfe einer vertrauenswürdigen Quell-IP-Adresse gefälscht wird, die von der angewendeten Zugriffsliste zugelassen ist.

Risikomanagement

Unternehmen wird empfohlen, ihre standardmäßigen Risikobewertungs- und Minderungsprozesse zu befolgen, um die potenziellen Auswirkungen von [dieser Schwachstelle|diesen Schwachstellen] zu ermitteln. Triage bezieht sich auf das Sortieren von Projekten und die Priorisierung von Bemühungen, die am wahrscheinlichsten erfolgreich sein werden. Cisco hat Dokumente bereitgestellt, die Unternehmen bei der Entwicklung einer risikobasierten Triage-Funktion für ihre Informationssicherheitsteams unterstützen. Risikoanalyse für Ankündigungen zu Sicherheitslücken sowie Risikoanalyse und -prototyping unterstützen Unternehmen bei der Entwicklung wiederholbarer Sicherheitsevaluierungs- und Reaktionsprozesse.

Gerätespezifische Eindämmung und Identifizierung

Spezifische Informationen zur Risikominderung und Identifizierung sind für diese Geräte verfügbar.

- Internet-Edge- und GRE-Terminierungsrouter
- VPN-Router
- Cisco ASA und PIX-Firewalls
- NetFlow

Internet-Edge- und GRE-Terminierungsrouter

Vorsicht: Die Effektivität der Risikominimierungstechnik hängt von spezifischen Kundensituationen wie Produktmix, Netzwerktopologie, Datenverkehrsverhalten und organisatorischem Auftrag ab. Prüfen Sie wie bei jeder Konfigurationsänderung die Auswirkungen dieser Konfiguration, bevor Sie die Änderung übernehmen.

Risikominderung: Schnittstellenzugriffsliste

Die folgende Zugriffsliste lässt IP-Protokollnummer 47 (GRE)-Pakete von einem einzigen bekannten Host (d. h. 192.0.2.1) zu, die für den IOS-Router selbst (d. h. 192.0.2.2) bestimmt sind. Alle anderen GRE-Pakete werden gefiltert.

Zusätzliche Zugriffslisteneinträge sollten als Teil einer Transit Access Control List implementiert werden, die den Transit- und Edge-Datenverkehr an den Netzwerkeingangspunkten filtert.

Weitere Informationen zu ACLs finden Sie unter Transit Access Control Lists: 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
```

Eindämmung: Anti-Spoofing

Diese Schwachstelle kann durch ein gefälschtes Paket ausgenutzt werden. Anti-Spoof-Schutz in Form von Unicast Reverse Path Forwarding kann bei ordnungsgemäßer Konfiguration nur eine begrenzte Eindämmung bieten. Diese Funktion sollte nicht als 100%ige Abwehr dienen, da gefälschte Pakete immer noch über die von uRPF erwartete oder von Anti-Spoofing-Zugriffslisten zugelassene Schnittstelle in das Netzwerk gelangen können. Außerdem muss darauf geachtet werden, dass der entsprechende uRPF-Modus (flexibel oder strikt) konfiguriert wird, um sicherzustellen, dass legitime Pakete nicht verworfen werden.

Weitere Informationen zur Unicast Reverse Path Forwarding finden Sie unter http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ft_urpf.html.

Eindämmung: GRE-Tunnel-ID

Die Verwendung eines Tunnelkennungsschlüssels kann dieses Problem möglicherweise beheben, aber der Befehl ist nicht als Sicherheitsfunktion gedacht, und der Schlüssel kann durch das Ermitteln legitimer GRE-Pakete gefunden werden. Weitere Informationen zu dieser Funktion finden Sie unter Configuring Logical Interfaces - Configuring a Tunnel Identification Key.

Auf dem Supervisor 720 werden GRE-Tunnel, die einen ID-Schlüssel verwenden, in einer Software verarbeitet, die sich auf die Leistung auswirken kann.

Identifikation

Nachdem die Schnittstellenzugriffsliste auf die GRE-Eingangsschnittstelle angewendet wurde, kann die Anzahl der gefilterten Pakete mit dem Befehl **show access-list <*acl number*>** identifiziert werden. Gefilterte Pakete sollten untersucht werden, um festzustellen, ob es sich um Versuche handelt, dieses Problem auszunutzen. Nachfolgend finden Sie ein Beispiel für die Ausgabe von **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
```

Im obigen Beispiel wurden 100 GRE-Pakete von der Zugriffsliste verworfen, die für "inbound" (Eingehend) an der Schnittstelle Ethernet 0/0 konfiguriert wurde.

VPN-Router

Vorsicht: Die Effektivität der Risikominimierungstechnik hängt von spezifischen Kundensituationen wie Produktmix, Netzwerktopologie, Datenverkehrsverhalten und organisatorischem Auftrag ab. Prüfen Sie wie bei jeder Konfigurationsänderung die Auswirkungen dieser Konfiguration, bevor Sie die Änderung übernehmen.

Eindämmung: GRE durch IPSec geschützt

Die Verschlüsselung von GRE-Tunneln mit IPSec ist das wirksamste Mittel zur Verhinderung von Angriffen. Weitere Informationen zur Verschlüsselung von GRE mit IPSec finden Sie in den folgenden Ressourcen:

- Konfigurieren eines GRE-Tunnels über IPSec mit OSPF
- Konfigurieren von IPSec/GRE mit NAT
- GRE over IPSec mit EIGRP zur Weiterleitung durch einen Hub und mehrere Remote-Standorte - Konfigurationsbeispiel
- Konfigurieren von Router-to-Router IPSec (Pre-shared Keys) im GRE-Tunnel mit CBAC und NAT

Risikominderung: Schnittstellenzugriffsliste

Die folgende Zugriffsliste filtert die IP-Protokollnummer 47 (GRE) von allen Hosts. VPN-Router, die in IPSec gekapselte GRE beenden, sollten keine unverschlüsselten GRE-Pakete an der physischen Eingangsschnittstelle empfangen.

Zusätzliche Zugriffslisteneinträge sollten als Teil einer Transit Access Control List implementiert werden, die den Transit- und Edge-Datenverkehr an den Netzwerkeingangspunkten filtert.

Weitere Informationen zu ACLs finden Sie unter Transit Access Control Lists: Filtering at Your Edge.

Die folgende Zugriffsliste erlaubt IPSec-Datenverkehr von einem einzigen vertrauenswürdigen Host (d. h. 192.0.2.1), der für den IPSec-Terminierungsrouter selbst (d. h. 192.0.2.2) bestimmt ist.

```
!-- 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
```

Die Schnittstellenzugriffsliste benötigt möglicherweise eine bestimmte Zugriffsliste, um GRE-Pakete von der IP-Adresse der GRE-Tunnelquelle in die IP-Adresse des GRE-Tunnelziels einzugeben, wenn die auf dem Gerät ausgeführte IOS-Version nicht die Korrektur für die Cisco Bug-ID CSCdu58486 aufweist (nur registrierte Kunden).

Eindämmung: GRE-Tunnel-ID

Die Verwendung eines Tunnelkennungsschlüssels kann dieses Problem möglicherweise beheben,

aber der Befehl ist nicht als Sicherheitsfunktion gedacht, und der Schlüssel kann durch das Ermitteln legitimer GRE-Pakete gefunden werden. Weitere Informationen zu dieser Funktion finden Sie unter Configuring Logical Interfaces - Configuring a Tunnel Identification Key.

Identifikation

Nachdem die Transit-Zugriffsliste auf die physische Eingangsschnittstelle angewendet wurde, kann mit dem Befehl **show access-list <*acl number*>** die Anzahl der gefilterten Pakete identifiziert werden. Gefilterte Pakete sollten untersucht werden, um festzustellen, ob es sich dabei um Versuche handelt, diese Schwachstelle auszunutzen. Nachfolgend finden Sie ein Beispiel für die Ausgabe von **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
```

Im obigen Beispiel wurden 100 GRE-Pakete von der Zugriffsliste verworfen, die für "inbound" (Eingehend) an der Schnittstelle Ethernet 0/0 konfiguriert wurde.

Cisco ASA und PIX-Firewalls

Vorsicht: Die Effektivität der Risikominimierungstechnik hängt von spezifischen Kundensituationen wie Produktmix, Netzwerktopologie, Datenverkehrsverhalten und organisatorischem Auftrag ab. Prüfen Sie wie bei jeder Konfigurationsänderung die Auswirkungen dieser Konfiguration, bevor Sie die Änderung übernehmen.

Eindämmung

Die folgenden Zugriffslisten lassen IP-Protokollnummer 47 (GRE)-Pakete von einem einzigen vertrauenswürdigen Host (d. h. 192.0.2.1) zu, die für den IOS-Router bestimmt sind, der GRE terminiert (d. h. 192.0.2.2). Alle anderen GRE-Pakete werden gefiltert.

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
```

Konfigurationsbeispiel zu PIX/ASA 7.x

Lassen Sie als Transitgerät nur vertrauenswürdige Quell-IP-Adressen GRE-Pakete an Geräte innerhalb der Firewall zu.

```
!-- 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
```

Identifikation

PIX 6.x

In diesem Beispiel wurden 100 GRE-Pakete empfangen und blockiert.

```
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)
```

Konfigurationsbeispiel zu PIX/ASA 7.x

In diesem Beispiel wurden 100 GRE-Pakete empfangen und blockiert.

```
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)
```

Wenn GRE in PIX/ASA 7.x über die Firewall zugelassen wird, muss der Befehl **show conn | include GRE** kann verwendet werden, um die spezifischen GRE-Verbindungen zu überprüfen, die die Firewall passieren. Unerwartete hergestellte GRE-Verbindungen sollten untersucht werden, um festzustellen, ob es sich um Versuche handelt, dieses Problem auszunutzen. Das nachfolgende Beispiel zeigt die Ausgabe für **show conn: | GRE einschließen**:

```
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

NetFlow kann auf Internet Edge- und GRE-Terminierungsroutern konfiguriert werden, um festzustellen, ob Versuche unternommen werden, diese Schwachstelle auszunutzen.

```
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 ----------
```

Im obigen Beispiel gibt es eine sehr hohe Anzahl von GRE (Protocol Hex 2F)-Flows von einer einzelnen IP-Adresse zu mehreren Ziel-IP-Adressen. Bei Internet-Edge-Routern und möglicherweise bei GRE-Terminierungsroutern kann dies auf einen Versuch hindeuten, diese Schwachstelle auszunutzen, und es sollte mit der Basisnutzung dieser Ports auf den Überwachungsgeräten verglichen werden.

Um nur GRE (Protocol Hex 2F)-Datenflüsse anzuzeigen, wird der Befehl **show ip cache flow | inc SrcIf|2F** kann wie folgt verwendet werden:

```
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 ----------
```

Zusätzliche Informationen

Dieses Dokument wird in der vorliegenden Form bereitgestellt und impliziert keine Garantie oder

Gewährleistung, einschließlich der Gewährleistung der Marktgängigkeit oder Eignung für einen bestimmten Zweck. Die Nutzung der Informationen im Dokument oder den Materialien, die mit dem Dokument verknüpft sind, erfolgt auf Ihr eigenes Risiko. Cisco behält sich das Recht vor, dieses Dokument jederzeit zu ändern oder zu aktualisieren.

Revisionsverlauf

Version 1.0	12. September 2006	Erste Veröffentlichung.

Cisco Sicherheitsverfahren

Vollständige Informationen zur Meldung von Sicherheitslücken in Cisco Produkten, zum Erhalt von Unterstützung bei Sicherheitsvorfällen und zur Registrierung für den Erhalt von Sicherheitsinformationen von Cisco finden Sie auf der weltweiten Cisco Website unter https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html. Dies beinhaltet Anweisungen für Presseanfragen bezüglich der Sicherheitshinweise von Cisco. Alle Cisco Sicherheitsankündigungen finden Sie unter http://www.cisco.com/go/psirt.

Zugehörige Informationen

- Erhöhung der Sicherheit auf Cisco Routern - Sicherung von IP-Routing
- RFC 2827: Network Ingress Filtering: Abwehr von Denial-of-Service-Angriffen mit IP Source Address Spoofing
- Unicast Reverse Path Forwarding Loose Mode
- Konfigurieren der IPSec-Netzwerksicherheit
- Konfigurieren eines GRE-Tunnels über IPSec mit OSPF
- Konfigurieren von IPSec/GRE mit NAT
- GRE over IPSec mit EIGRP zur Weiterleitung durch einen Hub und mehrere Remote-Standorte - Konfigurationsbeispiel
- Konfigurieren von Router-to-Router IPSec (Pre-shared Keys) im GRE-Tunnel mit CBAC und NAT

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.