Vaststelling en beperking van de exploitatie van de GRE-decapulatiekwetsbaarheid

Vaststelling en beperking van de exploitatie van de GRE-decapulatiekwetsbaarheid

Advies-ID: cisco-amb-20060912-gre

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

Revisie 1.0

Openbare publicatie 2006 September 12 17:00 UTC (GMT)

Inhoud

Cisco Response

Kwetsbaarheid Kenmerken

De kwetsbaarheid van Cisco IOS GRE-decapsulatie kan op afstand worden geëxploiteerd zonder verificatie en er is geen gebruikersinteractie nodig. Indien geëxploiteerd, kan de aanvaller Cisco IOS?-software veroorzaken om speciaal vervaardigde IPv4-pakketten door te sturen die mogelijk kunnen worden gebruikt om toegangscontrolelijsten te omzeilen. De aanvalsvector is via IP-protocol 47, Generic Routing Encapsulation (GRE). Deze kwetsbaarheid wordt niet gedekt door een CVE-id.

Dit document bevat informatie om Cisco-klanten te helpen bij pogingen om de kwetsbaarheid van Cisco IOS GRE-decapulatie te exploiteren. Deze kwetsbaarheid beïnvloedt apparaten die Cisco IOS-software uitvoeren die met GRE-tunnels is geconfigureerd. Zoals oorspronkelijk gedefinieerd in RFC1701, bevat het veld GRE Header een aantal vlagbits die zijn afgekeurd door RFC2784. Versies van Cisco IOS-software die RFC2784 ondersteunen, worden niet beïnvloed door deze kwetsbaarheid.

Kwetsbare, niet-getroffen en vaste software informatie is beschikbaar in de PSIRT Security Response:

Cisco Security Response to: Cisco IOS GRE-decapulatiekwetsbaarheid

Overzicht Mitigation Technique

Cisco-apparaten bieden verschillende tegenmaatregelen voor de kwetsbaarheid van Cisco IOS GRE-decapulatie. Tunnelbescherming in de vorm van IPSec-inkapseling is het meest effectieve middel om aanvallen te beperken. Deze aanval kan ook worden verzacht door een toegangslijst toe te passen in de inkomende richting van GRE-verkeer en het GRE-protocol te filteren van alle behalve vertrouwde bronadressen. Opgemerkt moet worden dat een aanval nog steeds succesvol kan zijn als het GRE-pakket wordt gespoofed met behulp van een vertrouwd bron-IP-adres dat is toegestaan door de toegepaste toegangslijst.

Risicobeheer

Organisaties wordt aangeraden om hun standaardprocessen voor risico-evaluatie en -beperking te volgen om de potentiële impact van [deze kwetsbaarheid|deze kwetsbaarheden] te bepalen. Triage verwijst naar het sorteren van projecten en het prioriteren van inspanningen die waarschijnlijk het meest succesvol zullen zijn. Cisco heeft documenten geleverd die organisaties kunnen helpen bij de ontwikkeling van een op risico gebaseerde triagecapaciteit voor hun informatieveiligheidsteams. Risico Triage voor Security Vulnerability aankondigingen en Risk Triage en Prototyping kunnen organisaties helpen herhaalbare security evaluatie- en reactieprocessen te ontwikkelen.

Apparaatspecifieke beperking en identificatie

Voor deze hulpmiddelen is specifieke informatie over beperking en identificatie beschikbaar

- Internet Edge- en GRE-afsluitrouters
- VPN-routers
- Cisco ASA- en PIX-firewalls
- NetFlow

Internet Edge- en GRE-afsluitrouters

Waarschuwing: de effectiviteit van elke mitigatietechniek is afhankelijk van specifieke klantsituaties zoals productmix, netwerktopologie, verkeersgedrag en organisatorische missie. Zoals bij elke configuratiewijziging, evalueer het effect van deze configuratie voordat u de wijziging toepast.

Beperking: interfacetoegangslijst

De volgende toegangslijst maakt IP-protocolnummer 47 (GRE) pakketten mogelijk van één bekende host (bijv. 192.0.2.1) en bestemd voor de IOS-router zelf (bijv. 192.0.2.2). Alle andere GRE-pakketten worden gefilterd.

Toegevoegde toegangslijstvermeldingen moeten worden geïmplementeerd als onderdeel van een Transit Access Control List waarmee doorvoer- en randverkeer op netwerktoegangspunten wordt

gefilterd.

Raadpleeg voor meer informatie over ACL's 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
```

Beperken: anti-spoofing

Deze kwetsbaarheid kan worden uitgebuit door een spoofed-pakket. Anti-nep bescherming in de vorm van unicast omgekeerd pad doorsturen kan beperkte beperking bieden indien goed geconfigureerd. Op deze voorziening mag niet worden vertrouwd om 100% beperking te bieden, aangezien spoofed-pakketten nog steeds het netwerk kunnen binnendringen via de interface die door uRPF wordt verwacht of die is toegestaan door toegangslijsten tegen spoofing. Er moet ook voor gezorgd worden dat de juiste uRPF-modus (losjes of strikt) zo geconfigureerd is dat legitieme pakketten niet verloren gaan.

Aanvullende informatie over unicast Reverse Path Forwarding is beschikbaar op http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ft_urpf.html.

Beperking: GRE-tunnelid

Het toepassen van een tunnel-ID-sleutel kan enige verlichting bieden tegen dit probleem, maar de opdracht is niet bedoeld als een beveiligingsfunctie en de sleutel kan worden gevonden door het snuiven van legitieme GRE-pakketten. Raadpleeg voor meer informatie over deze functie Configureren van logische interfaces - Een tunnelidentificatiesleutel configureren.

Op de Supervisor 720 worden GRE-tunnels met een ID-toets verwerkt in software die van invloed kan zijn op de prestaties.

Identificatie

Zodra de lijst van de interfacetoegang wordt toegepast op de GRE ingangsinterface, **toont** het bevel **toegang-lijst <*acl number*>** kan worden gebruikt om het aantal pakketten te identificeren die worden gefilterd. Gefilterde pakketten moeten worden onderzocht om te bepalen of ze pogingen zijn om dit probleem te exploiteren. Na is voorbeeldoutput voor **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
```

In het bovenstaande voorbeeld zijn 100 GRE-pakketten gevallen door de toegangslijst die is geconfigureerd op interface Ethernet 0/0.

VPN-routers

Waarschuwing: de effectiviteit van elke mitigatietechniek is afhankelijk van specifieke klantsituaties zoals productmix, netwerktopologie, verkeersgedrag en organisatorische missie. Zoals bij elke configuratiewijziging, evalueer het effect van deze configuratie voordat u de wijziging toepast.

Beperking: GRE, beschermd door IPSec

Het versleutelen van GRE-tunnels met IPSec is het meest effectieve middel om aanvallen te voorkomen. Raadpleeg deze bronnen voor aanvullende informatie over het versleutelen van GRE met IPSec:

- Een GRE-tunnel via IPSec met OSPF configureren
- IPsec/GRE configureren met NAT
- GRE over IPSec met EIGRP naar router via een hub en configuratievoorbeeld van meerdere externe locaties
- Het configureren van router-naar-router IPSec (vooraf gedeelde sleutels) op GRE-tunnel met CBAC en NAT

Beperking: interfacetoegangslijst

De volgende toegangslijst filtert IP-protocolnummer 47 (GRE) van alle hosts. VPN-routers die GRE inkapselen in IPSec mogen geen duidelijke tekst (niet-versleuteld) GRE-pakketten ontvangen op de fysieke toegangsinterface.

Toegevoegde toegangslijstvermeldingen moeten worden geïmplementeerd als onderdeel van een Transit Access Control List waarmee doorvoer- en randverkeer op netwerktoegangspunten wordt gefilterd.

Raadpleeg voor meer informatie over ACL's Transit Access Control Lists: filtering at Your Edge.

De volgende toegangslijst maakt verkeer van IPSec mogelijk vanaf één vertrouwde host (d.w.z. 192.0.2.1) en bestemd voor de IPSec-terminerende router zelf (d.w.z. 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
```

De toegangslijst met interfaces heeft mogelijk een specifieke toegangslijst nodig voor het verlenen van vergunningen voor GRE-pakketten van het IP-adres van de GRE-tunnelbron naar het IP-adres van de GRE-tunnelbestemming als de IOS-versie die op het apparaat wordt uitgevoerd niet de oplossing heeft voor Cisco-bug-id CSCdu58486 (alleen geregistreerde klanten).

Beperking: GRE-tunnelid

Het toepassen van een tunnel-ID-sleutel kan enige verlichting bieden tegen dit probleem, maar de opdracht is niet bedoeld als een beveiligingsfunctie en de sleutel kan worden gevonden door het snuiven van legitieme GRE-pakketten. Raadpleeg voor meer informatie over deze functie

Configureren van logische interfaces - Een tunnelidentificatiesleutel configureren.

Identificatie

Zodra de transittoegangslijst is toegepast op de fysieke toegangsinterface, **toont** de opdracht **toegang-lijst <*acl number*>**kan worden gebruikt om het aantal pakketten te identificeren die worden gefilterd. Gefilterde pakketten zouden moeten worden onderzocht om te bepalen als zij pogingen zijn om deze kwetsbaarheid te exploiteren. Na is voorbeeldoutput voor **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
```

In het bovenstaande voorbeeld zijn 100 GRE-pakketten gevallen door de toegangslijst die is geconfigureerd op interface Ethernet 0/0.

Cisco ASA- en PIX-firewalls

Waarschuwing: de effectiviteit van elke mitigatietechniek is afhankelijk van specifieke klantsituaties zoals productmix, netwerktopologie, verkeersgedrag en organisatorische missie. Zoals bij elke configuratiewijziging, evalueer het effect van deze configuratie voordat u de wijziging toepast.

Beperken

De volgende toegangslijsten maken IP-protocolnummer 47 (GRE) pakketten mogelijk van één vertrouwde host (bijv. 192.0.2.1) en zijn bestemd voor de IOS-router die GRE (d.w.z. 192.0.2.2). Alle andere GRE-pakketten worden gefilterd.

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

Als een transitapparaat, staat alleen vertrouwde bron IP-adressen toe om GRE-pakketten naar apparaten binnen de firewall te verzenden.

```
!-- 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
```

Identificatie

PIX 6.x

In dit voorbeeld zijn 100 GRE-pakketten ontvangen en geblokkeerd.

```
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

In dit voorbeeld zijn 100 GRE-pakketten ontvangen en geblokkeerd.

```
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, als GRE door de firewall is toegestaan, **toont** de opdracht **conn | met inbegrip van GRE** kan worden gebruikt om de specifieke GRE-verbindingen te verifiëren die door de firewall lopen. Onverwachte gevestigde GRE-verbindingen moeten worden onderzocht om te bepalen of ze pogingen zijn om van dit probleem te profiteren. Na is voorbeelduitvoer voor **show conn | 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

NetFlow kan worden geconfigureerd op Internet Edge en GRE-terminatierouters om te bepalen of er pogingen worden ondernomen om deze kwetsbaarheid te benutten.

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

In het bovenstaande voorbeeld is er een zeer groot aantal GRE (Protocol Hex 2F)-stromen van één IP-adres naar meerdere IP-adressen van bestemmingen. Op Internet-randrouters en mogelijk op GRE-terminatierouters kan dit een indicatie zijn van een poging om deze kwetsbaarheid te exploiteren en moet dit worden vergeleken met het basislijngebruik van deze poorten op de bewakingsapparaten.

Als u alleen GRE-stromen (Protocol Hex 2F) wilt weergeven, **toont** de opdracht **IP cache flow | inc SrcIndien|2F** kan worden gebruikt zoals hieronder aangegeven:

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

Aanvullende informatie

WIJZIGEN OF TE ANNULEREN.

Revisiegeschiedenis

Revisie 1.0	2006-12 september	Eerste publieke publicatie.

Cisco-beveiligingsprocedures

Volledige informatie over het melden van beveiligingskwetsbaarheden in Cisco-producten, het verkrijgen van assistentie bij beveiligingsincidenten en het registreren om beveiligingsinformatie van Cisco te ontvangen, is beschikbaar op de wereldwijde website van Cisco op https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html. Dit omvat instructies voor persvragen over Cisco-beveiligingsmeldingen. Alle Cisco-beveiligingsadviezen zijn beschikbaar op http://www.cisco.com/go/psirt.

Gerelateerde informatie

- Beveiliging op Cisco-routers verbeteren - IP-routing beveiligen
- RFC 2827: Network Ingress Filtering: Verslaan Denial of Service-aanvallen die IP-bronadresspoofing gebruiken
- Unicast omgekeerde pad doorsturen in losse modus
- IPsec-netwerkbeveiliging configureren
- Een GRE-tunnel via IPSec met OSPF configureren
- IPsec/GRE configureren met NAT
- GRE over IPSec met EIGRP naar router via een hub en configuratievoorbeeld van meerdere externe locaties
- Het configureren van router-naar-router IPSec (vooraf gedeelde sleutels) op GRE-tunnel met CBAC en NAT

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.