GRE 역캡슐화 취약성 익스플로잇 식별 및 완화

GRE 역캡슐화 취약성 익스플로잇 식별 및 완화

자문 ID: cisco-amb-20060912-gre

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

개정 1.0

2006년 9월 12일 17:00 UTC(GMT) 공개 릴리스의 경우

목차

Cisco의 대응

취약성 특성

Cisco IOS GRE 역캡슐화 취약성은 인증 없이 원격으로 악용될 수 있으며 사용자 상호 작용이 필요하지 않습니다. 공격자가 공격을 받는 경우 Cisco IOS? 소프트웨어에서 특별히 제작한 IPv4 패킷을 전달하게 할 수 있으며, 이는 잠재적으로 액세스 제어 목록을 우회하는 데 사용될 수 있습니다. 공격 벡터는 IP 프로토콜 47, GRE(Generic Routing Encapsulation)를 통해 이루어집니다. 이 취약성은 CVE ID에 포함되지 않습니다.

이 문서에는 Cisco 고객이 Cisco IOS GRE 역캡슐화 취약성을 악용하려는 시도를 완화하는 데 도움이 되는 정보가 포함되어 있습니다. 이 취약성은 GRE 터널로 구성된 Cisco IOS 소프트웨어를 실행하는 디바이스에 영향을 미칩니다. 원래 RFC1701에 정의된 대로, GRE 헤더 필드에는 RFC2784에서 더 이상 사용되지 않는 플래그 비트 수가 포함됩니다. RFC2784를 지원하는 Cisco IOS 소프트웨어 버전은 이 취약성의 영향을 받지 않습니다.

PSIRT Security Response(PSIRT 보안 대응)에서 취약하고 영향을 받지 않으며 고정된 소프트웨어 정보를 이용할 수 있습니다.

Cisco Security Response to: Cisco IOS GRE 역캡슐화 취약성

완화 기법 개요

Cisco 디바이스는 Cisco IOS GRE 역캡슐화 취약성에 대한 몇 가지 대응책을 제공합니다. IPSec 캡

술화 형태의 터널 보호는 가장 효과적인 공격 완화 방법입니다. 또한 GRE 트래픽의 인바운드 방향으로 액세스 목록을 적용하고 신뢰할 수 있는 소스 주소를 제외한 모든 주소에서 GRE 프로토콜을 필터링하여 이 공격을 완화할 수 있습니다. 적용된 액세스 목록에서 허용하는 신뢰할 수 있는 소스 IP 주소를 사용하여 GRE 패킷을 스푸핑하면 공격이 여전히 성공할 수 있습니다.

위험 관리

조직은 표준 위험 평가 및 완화 프로세스를 준수하여 [이 취약성|이러한 취약성]의 잠재적 영향을 확인하는 것이 좋습니다. 분류(Triage)란 성공 가능성이 가장 높은 프로젝트를 분류하고 노력을 우선순위를 정하는 것을 말한다. Cisco는 조직이 정보 보안 팀을 위해 위험 기반 분류 기능을 개발하는 데 도움이 될 문서를 제공했습니다. 보안 취약성 알림에 대한 위험 분류 및 위험 분류 및 프로토타이핑은 조직이 반복 가능한 보안 평가 및 대응 프로세스를 개발하는 데 도움이 될 수 있습니다.

디바이스별 완화 및 식별

차단 및 식별에 대한 구체적인 정보를 이러한 장치에 사용할 수 있습니다.

- 인터넷 에지 및 GRE 종단 라우터
- VPN 라우터
- Cisco ASA 및 PIX 방화벽
- Netflow

인터넷 에지 및 GRE 종단 라우터

주의: 어떤 완화 기술이든 효과는 제품 혼합, 네트워크 토폴로지, 트래픽 동작, 조직 임무 등 특정 고객 상황에 따라 달라집니다. 모든 컨피그레이션 변경과 마찬가지로, 변경 사항을 적용하기 전에 이 컨피그레이션의 영향을 평가합니다.

완화: 인터페이스 액세스 목록

다음 액세스 목록은 알려진 단일 호스트(예: 192.0.2.1)에서 IOS 라우터 자체(예: 192.0.2.2)로 전달되는 IP 프로토콜 번호 47(GRE) 패킷을 허용합니다. 다른 모든 GRE 패킷은 필터링됩니다.

추가된 액세스 목록 항목은 네트워크 인그레스 포인트에서 전송 및 에지 트래픽을 필터링하는 전송 액세스 제어 목록의 일부로 구현되어야 합니다.

ACL에 대한 자세한 내용은 Transit Access Control Lists: Filtering at Your Edge를 참조하십시오.

```
!-- 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
```

완화: 스푸핑 차단

이 취약성은 스푸핑된 패킷에 의해 악용될 수 있습니다. 유니캐스트 Reverse Path Forwarding 형식의 안티스푸핑 보호는 올바르게 구성된 경우 제한적인 완화 기능을 제공할 수 있습니다. 스푸핑된 패킷은 uRPF에서 예상하거나 스푸핑 차단 액세스 목록에서 허용하는 인터페이스에서 네트워크에 계속 들어올 수 있으므로 이 기능을 100% 완화를 제공하기 위해 사용하면 안 됩니다. 또한 적절한 uRPF 모드(느슨하거나 엄격함)가 구성되어 합법적인 패킷이 삭제되지 않도록 해야 합니다.

유니캐스트 Reverse Path Forwarding에 대한 추가 정보는 http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ft_urpf.html에서 확인할 수 있습니다.

완화: GRE 터널 ID

터널 ID 키를 적용하면 이 문제를 어느 정도 완화할 수 있지만 이 명령은 보안 기능으로 사용되지 않으며 합법적인 GRE 패킷을 스니핑하여 키를 찾을 수 있습니다. 이 기능에 대한 자세한 내용은 논리적 인터페이스 구성 - 터널 식별 키 구성을 참조하십시오.

수퍼바이저 720에서는 ID 키를 사용하는 GRE 터널이 소프트웨어로 처리되어 성능에 영향을 줄 수 있습니다.

식별

인터페이스 액세스 목록이 GRE 인그레스 인터페이스에 적용되면 **show access-list <*acl number*> 명령**을 사용하여 필터링되는 패킷 수를 식별할 수 있습니다. 필터링된 패킷을 조사하여 이 문제를 악용하려는 시도인지 확인해야 합니다. 다음은 show access-**list 100의 출력 예입니다**.

```
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
```

위의 예에서는 인터페이스 Ethernet 0/0에서 인바운드로 구성된 액세스 목록에 의해 100개의 GRE 패킷이 삭제되었습니다.

VPN 라우터

주의: 어떤 완화 기술이든 효과는 제품 혼합, 네트워크 토폴로지, 트래픽 동작, 조직 임무 등 특정 고객 상황에 따라 달라집니다. 모든 컨피그레이션 변경과 마찬가지로, 변경 사항을 적용하기 전에 이 컨피그레이션의 영향을 평가합니다.

완화: IPSec으로 GRE 보호

IPSec으로 GRE 터널을 암호화하는 것이 가장 효과적인 공격 방지 수단입니다. IPSec으로 GRE를 암호화하는 방법에 대한 자세한 내용은 다음 리소스를 참조하십시오.

- OSPF를 사용하여 IPSec을 통한 GRE 터널 구성
- NAT로 IPSec/GRE 구성
- EIGRP를 사용하여 허브 및 여러 원격 사이트를 통해 라우팅하는 GRE over IPSec 컨피그레이션 예
- CBAC 및 NAT를 사용하여 GRE 터널에서 라우터 간 IPSec(사전 공유 키) 구성

완화: 인터페이스 액세스 목록

다음 액세스 목록은 모든 호스트에서 IP 프로토콜 번호 47(GRE)을 필터링합니다. IPSec에서 캡슐화된 GRE를 종료하는 VPN 라우터는 물리적 인그레스 인터페이스에서 일반 텍스트(암호화되지 않은) GRE 패킷을 수신하지 않아야 합니다.

추가된 액세스 목록 항목은 네트워크 인그레스 포인트에서 전송 및 에지 트래픽을 필터링하는 전송 액세스 제어 목록의 일부로 구현되어야 합니다.

ACL에 대한 자세한 내용은 Transit Access Control Lists: Filtering at Your Edge를 참조하십시오.

다음 액세스 목록은 신뢰할 수 있는 단일 호스트(예: 192.0.2.1)에서 오는 IPSec 트래픽을 허용하며, IPSec 종료 라우터 자체(예: 192.0.2.2)를 대상으로 합니다.

```
!-- 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
```

디바이스에서 실행 중인 IOS 버전에 Cisco 버그 ID CSCdu58486(등록된 고객만 해당)에 대한 수정 사항이 없는 경우 인터페이스 액세스 목록에는 GRE 터널 소스 IP 주소에서 GRE 터널 대상 IP 주소로의 GRE 패킷에 대한 특정 액세스 목록 허용 항목이 필요할 수 있습니다.

완화: GRE 터널 ID

터널 ID 키를 적용하면 이 문제를 어느 정도 완화할 수 있지만 이 명령은 보안 기능으로 사용되지 않으며 합법적인 GRE 패킷을 스니핑하여 키를 찾을 수 있습니다. 이 기능에 대한 자세한 내용은 논리적 인터페이스 구성 - 터널 식별 키 구성을 참조하십시오.

식별

트랜짓 액세스 목록이 물리적 인그레스 인터페이스에 적용되면 명령 **show access-list <*acl number*>를** 사용하여 필터링되는 패킷 수를 식별할 수 있습니다. 필터링된 패킷을 조사하여 이 취약성을 악용하려는 시도인지 확인해야 합니다. 다음은 show access-list 100의 출력 예입니다.

```
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
```

위의 예에서는 인터페이스 Ethernet 0/0에서 인바운드로 구성된 액세스 목록에 의해 100개의 GRE 패킷이 삭제되었습니다.

Cisco ASA 및 PIX 방화벽

주의: 어떤 완화 기술이든 효과는 제품 혼합, 네트워크 토폴로지, 트래픽 동작, 조직 임무 등 특정 고객 상황에 따라 달라집니다. 모든 컨피그레이션 변경과 마찬가지로, 변경 사항을 적용하기 전에 이 컨피그레이션의 영향을 평가합니다.

완화

다음 액세스 목록은 신뢰할 수 있는 단일 호스트(예: 192.0.2.1)에서 IP 프로토콜 번호 47(GRE) 패킷을 허용하며, GRE를 종료하는 IOS 라우터로 전달됩니다(예: 192.0.2.2). 다른 모든 GRE 패킷은 필터링됩니다.

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

트랜짓 디바이스에서는 신뢰할 수 있는 소스 IP 주소만 방화벽 내의 디바이스로 GRE 패킷을 전송하도록 허용합니다.

```
!-- 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
```

식별

PIX 6.x

이 예에서는 100개의 GRE 패킷이 수신 및 차단되었습니다.

```
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

이 예에서는 100개의 GRE 패킷이 수신 및 차단되었습니다.

```
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)
```

PIX/ASA 7.x에서 GRE가 방화벽을 통과할 수 있는 경우 명령 show conn을 **실행합니다 | include GRE**를 사용하여 방화벽을 통과하는 특정 GRE 연결을 확인할 수 있습니다. 예기치 않은 설정된 GRE 연결을 조사하여 이 문제를 악용하려는 시도인지 확인해야 합니다. 다음은 show conn에 대한 **출력입니다 | GRE 포함**:

```
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

Internet Edge 및 GRE 종단 라우터에서 NetFlow를 구성하여 이 취약성을 악용하려는 시도가 진행 중인지 확인할 수 있습니다.

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

위의 예에서는 단일 IP 주소에서 여러 목적지 IP 주소로 이동하는 매우 많은 GRE(Protocol Hex 2F) 흐름이 있습니다. 인터넷 에지 라우터 및 잠재적으로 GRE 종단 라우터에서 이는 이 취약성을 악용하려는 시도를 나타낼 수 있으며 모니터링 디바이스에서 이러한 포트의 기본 사용률과 비교해야 합니다.

GRE(Protocol Hex 2F) 흐름만 보려면 명령 show **ip cache flow | inc SrcIf|2F는** 다음 그림과 같이 사용할 수 있습니다.

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

추가 정보

개정 이력

개정 1.0	2006년 9월 12일	초기 공개 릴리스.

Cisco 보안 절차

Cisco 제품의 보안 취약성 보고, 보안 사고에 대한 지원 요청, Cisco의 보안 정보 수신을 위한 등록 등에 대한 자세한 내용은 Cisco의 전 세계 웹 사이트 (https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html)에서 확인할 수 있습니다. 여기에는 Cisco 보안 알림과 관련된 언론 문의에 대한 지침이 포함됩니다. 모든 Cisco 보안 권고 사항은 http://www.cisco.com/go/psirt에서 확인할 수 있습니다.

관련 정보

- Cisco 라우터의 보안 개선 - IP 라우팅 보안
- RFC 2827: 네트워크 인그레스 필터링: IP 소스 주소 스푸핑을 사용하는 서비스 거부 공격 방지
- 유니캐스트 역방향 경로 전달 느슨한 모드
- IPSec 네트워크 보안 구성
- OSPF를 사용하여 IPSec을 통한 GRE 터널 구성
- NAT로 IPSec/GRE 구성

- EIGRP를 사용하여 허브 및 여러 원격 사이트를 통해 라우팅하는 GRE over IPSec 컨피그레이션 예
- CBAC 및 NAT를 사용하여 GRE 터널에서 라우터 간 IPSec(사전 공유 키) 구성

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.