GRE 非カプセル化脆弱性の識別し、軽減不正利用

GRE 非カプセル化脆弱性の識別し、軽減不正利用

Advisory ID: cisco-amb-20060912-gre

http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20060912-gre

リビジョン 1.0

一般公開 2006 年に関しては 9月 12 17:00 UTC（GMT）

目次

Cisco の対応

脆弱性の特性

Cisco IOS GRE 非カプセル化脆弱性は認証無しでリモートで不正利用することができ、ユーザー操作は必要ではないです。 不正利用された場合、攻撃者により Cisco IOS を引き起こすかもしれませんか。 可能性としてはアクセスコントロールリストをバイパスするのに使用できる特に 巧妙に細工された IPv4 パケットを転送するソフトウェア。 攻撃 ベクトルは IP プロトコル 47 によって、総称ルーティング カプセル化（GRE）あります。 この脆弱性には CVE ID が割り当てられていません。

この資料は Cisco IOS GRE 非カプセル化脆弱性を不正利用する軽減試みの Cisco カスタマを支援するために情報が含まれています。 この脆弱性は GREトンネルで設定される実行するデバイス Cisco IOSソフトウェアに影響を与えます。 RFC1701 で最初に定義されるように、GRE ヘッダー フィールドは RFC2784 によって非難されたいくつかのフラグビットが含まれています。 Cisco IOSソフトウェアのバージョンはこの脆弱性から RFC2784 をサポートする影響を受けません。

脆弱 な、非影響を受けたおよび修正済みソフトウェア 情報は PSIRT セキュリティ応答で利用できます:

Ciscoセキュリティ応答への: Cisco IOS GRE 非カプセル化脆弱性

緩和テクニックの概要

Ciscoデバイスは Cisco IOS GRE 非カプセル化脆弱性に複数の対策を提供します。 IPSecカプセル化の形のトンネル 保護は攻撃軽減のほとんどの有効な手段です。 この攻撃はまた GRE トラフィックの受信方向のアクセス リストを追加することおよび信頼されたソース ソース· アドレスを除いたすべてから GRE プロトコルをフィルタリングすることによって軽減することができます。 GRE パケットが応用アクセス リストによって許可された信頼されたソース IP アドレスを使用してスプーフィングされる場合攻撃がまだ正常かもしれないことに注意する必要があります。

リスク管理

組織は潜在的影響をの判別するために標準リスク評価および軽減プロセスに従うように助言されます[この脆弱性|これらの脆弱性]。 トリアージとは、プロジェクトを分類して、成功する可能性が高い取り組みに優先順位を付けることです。 Cisco では、各組織の情報セキュリティ チームがリスクベースのトリアージを行う能力を身に着けるために役立つドキュメントを提供しています。 セキュリティーの脆弱性 お知らせのためのリスク トリアージはおよび リスク トリアージおよびプロトタイピング反復可能な機密 保護 評価および応答プロセスを開発するために組織を助けることができます。

デバイス別の緩和策と識別策

軽減および識別の特定の情報はこれらのデバイスで利用できます

- インターネットはルータ研ぎ、GRE 終了
- VPN ルータ
- Cisco ASA および PIXファイアウォール
- NetFlow

インターネット エッジおよび GRE 終了 ルータ

注意： 緩和テクニックの効果は、製品の組み合せ、ネットワーク トポロジ、トラフィックの動作、組織のミッションなど、お客様の状況によって異なります。 設定を変更する際には、変更を適用する前にその設定の影響を評価する必要があります。

緩和策： インターフェイス アクセス リスト

単一既知ホストからの次のアクセス リスト割り当て IP プロトコル第 47 （ GRE ）パケット（ すなわち、192.0.2.1 ）および IOSルータのために予定されて自体（ すなわち 192.0.2.2 ）。 他の GRE パケットはすべてフィルタ処理されたです。

追加されたアクセス リストエントリはフィルターおよびエッジ トラフィックがネットワークイングレスポイントで通過する中継アクセス制御リストの一部として設定されるはずです。

ACL に関する詳細については、中継をアクセス コントロール リスト（ ACL ）参照して下さい: エッジでのフィルタリング』を参照してください。

```
!-- 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
```

緩和策： アンチスプーフィング

この脆弱性はスプーフィングされたパケットによって不正利用することができます。 Unicast Reverse Path Forwarding の形の Anti-spoof 保護は正しく設定されたら限られた軽減を提供できます。 この機能はスプーフィングされたパケットがまだ uRPF によって期待されるか、またはアンチスプーフィング アクセスリストによって許可されるインターフェイスからネットワークに入るかもしれないので 100% 軽減を提供するために頼るべきではありません。 また、正当なパケットが廃棄されないように、適切な uRPF モード (loose または strict) を確実に設定するように注意する必要があります。

Unicast Reverse Path Forwarding についてのその他の情報は http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ft_urpf.html で利用できます。

緩和策： GREトンネル ID

トンネル ID キーをこの問題に対して軽減を提供するセキュリティ機能およびキーが正当 な GRE パケットのスニッフィングによって検索することができると同時にコマンドは意図されていません。 この機能に関する詳細については、論理インターフェイスの設定を-トンネル 識別 キーを設定すること参照して下さい。

スーパバイザ 720 で、ID キーを使用して GREトンネルはパフォーマンスに影響を与えるかもしれないソフトウェアで処理されます。

確認方法

インターフェイス アクセス リストが GRE 入力 インターフェイスに追加されれば、コマンド **show access-list <acl *数が* >** フィルタリングされるパケットの数を確認するのに使用することができます。 フィルタ処理されたパケットはこの問題を不正利用する試みだったかどうか確認するために調査する必要があります。 以下は **show access-list 100** のための出力例です:

```
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
```

上の例では、100 つの GRE パケットはインターフェイス イーサネット 0/0 のアクセス リストによって設定される受信によって廃棄されました。

VPN ルータ

注意： 緩和テクニックの効果は、製品の組み合せ、ネットワーク トポロジ、トラフィックの動作、組織のミッションなど、お客様の状況によって異なります。 設定を変更する際には、変更を適用する前にその設定の影響を評価する必要があります。

緩和策： IPSec によって保護される GRE

IPSec の GREトンネルを暗号化することは攻撃防止のほとんどの有効な手段です。 IPSec の GRE の暗号化についてのその他の情報に関しては、これらのリソースを参照して下さい:

- OSPF を使用した GRE トンネル over IPSec の設定
- NAT を使用する IPSec/GRE の設定
- ハブと複数のリモート サイトの設定例を使用してパスを指定する EIGRP での GRE over IPsec
- CBAC およびNAT を使用する GREトンネルの Router-to-Router IPSec （事前共有キー）の設定

緩和策： インターフェイス アクセス リスト

すべてのホストからの次のアクセス リスト フィルター IP プロトコル第 47 （GRE）。 IPSec でカプセル化される GRE を終える VPN ルータは物理的 な 入力 インターフェイスのクリアテキスト（非暗号化）GRE パケットを受信するべきではありません。

追加されたアクセス リストエントリはフィルターおよびエッジ トラフィックがネットワークイングレスポイントで通過する中継アクセス制御リストの一部として設定されるはずです。

ACL に関する詳細については、中継をアクセス コントロール リスト（ACL）参照して下さい: エッジでのフィルタリング』を参照してください。

単一 信頼できるホストからの次のアクセス リスト割り当て IPSecトラフィック（すなわち、192.0.2.1）および IPSec 終端ルータのために予定されて自体（すなわち、192.0.2.2）。

```
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
```

インターフェイス アクセス リストはデバイスで動作する IOSバージョンに Cisco バグ ID CSCdu58486 （登録ユーザのみ）のための修正がない場合 GREトンネル ソース IP アドレスからの GREトンネル 宛先 IP アドレスに GRE パケットのための特定のアクセス リスト割り当てエントリを必要とする場合もあります。

緩和策： GREトンネル ID

トンネル ID キーをこの問題に対して軽減を提供するセキュリティ機能およびキーが正当 な GRE パケットのスニッフィングによって検索することができると同時にコマンドは意図されていません。 この機能に関する詳細については、論理インターフェイスの設定を-トンネル 識別 キーを設定すること参照して下さい。

確認方法

中継アクセス リストが物理的 な 入力 インターフェイスに追加されれば、コマンド **show access-list <acl *数が* >** フィルタリングされるパケットの数を確認するのに使用することができます。 フィルタ処理されたパケットはこの脆弱性を不正利用する試みだったかどうか確認するために調査する必要があります。 以下は **show access-list 100** のための出力例です:

```
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
```

上の例では、100 つの GRE パケットはインターフェイス イーサネット 0/0 のアクセス リストによって設定される受信によって廃棄されました。

Cisco ASA および PIXファイアウォール

注意： 緩和テクニックの効果は、製品の組み合せ、ネットワーク トポロジ、トラフィックの動作、組織のミッションなど、お客様の状況によって異なります。 設定を変更する際には、変更を適用する前にその設定の影響を評価する必要があります。

緩和策

単一 信頼できるホストからの次のアクセス リスト割り当て IP プロトコル第 47 （ GRE ）パケット（ すなわち、192.0.2.1 ）および終える IOSルータのために予定されて GRE を（ すなわち。 192.0.2.2 ）。 他の GRE パケットはすべてフィルタ処理されたです。

PIX 6.x

```
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
```

PIX/ASA 7.x

中継デバイスとして、ファイアウォールのの中のデバイスに GRE パケットを送信する割り当て信頼されたソース IP アドレスだけ。

```
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
```

確認方法

PIX 6.x

この例では、100 つの GRE パケットは受信され、ブロックされました。

```
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

この例では、100 つの GRE パケットは受信され、ブロックされました。

```
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.x では、GRE がファイアウォールによって許可されれば、コマンド **show conn | GRE をファイアウォールによって通過する仕様 GRE 接続を確認するのに使用することができます含んで下さい。** 予想外確立された GRE 接続はこの問題を不正利用する試みだったかどうか確認するために調査する必要があります。 以下は **show conn のための出力例です | GRE を含んで下さい**:

```
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 はインターネット エッジおよび GRE 終了 ルータでこの脆弱性を不正利用するために試みが進行中だったかどうか確認するために設定することができます。

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

上の例では、単一 IP アドレスから複数のデスティネーション IP アドレスへの非常に多くの GRE（プロトコル Hex 2F）フローがあります。 のインターネット エッジルータと可能性としては GRE 終了 ルータ、これはこの脆弱性を不正利用する試みを表すかもしれ、モニタリング デバイスのこれらのポートのベースライン 利用と比較する必要があります。

GRE（プロトコル Hex 2F）フローしか表示しないため、コマンド **show ip cache flow | 株式会社 SrcIf|2F は**ここに示されているように使用されるかもしれません:

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

追加情報

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

改訂履歴

リビジョン 1.0	2006-September-12	初回公開リリース

Ciscoセキュリティ手順

セキュリティ上の問題の支援を得、Cisco からセキュリティ情報を受け取るために登録するシスコ製品のレポート セキュリティーの脆弱性の完全情報は http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html で Cisco の Worldwide Web サイトで利用できます。 これには Ciscoのセキュリティの告知に関する報道関係からの問い合わせのための手順が含まれています。 すべての Cisco セキュリティ アドバイザリは、http://www.cisco.com/go/psirt から入手できます。

関連情報

- セキュリティ ルータ on Cisco 改良します- IP ルーティングの保護
- RFC 2827: ネットワーク入口 フィルタリング: IPソースアドレス スプーフィングを用いる不正侵入を Denial of Service (DoS/DDoS) 阻止します
- Unicast Reverse Path Forwarding の Loose モード (英語)
- IPsec ネットワーク セキュリティの設定
- OSPF を使用した GRE トンネル over IPSec の設定
- NAT を使用する IPSec/GRE の設定
- ハブと複数のリモート サイトの設定例を使用してパスを指定する EIGRP での GRE over IPsec
- CBAC およびNAT を使用する GREトンネルの Router-to-Router IPSec （ 事前共有キー ） の設定