OSPF、MPLS VPN およびスーパバイザ 32、スーパバイザ 720、または Route Switch Processor 720 の Cisco IOS の脆弱性

High

アドバイザリーID : cisco-sa-20080326-queue

初公開日 : 2008-03-26 16:00

バージョン 1.3 : Final

CVSSスコア : 7.8

回避策 : No Workarounds available

Cisco バグ ID : CSCsf12082

CVE-2008-0537

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

12.2 に基づいて Cisco IOS のブランチを実行するある特定の Cisco Catalyst 6500 シリーズおよび Cisco 7600 ルータ デバイスはどのトラフィックでも影響を受けたインターフェイスに入ることを防ぐことができるサービス拒否の脆弱性に脆弱である場合もあります。 脆弱であるデバイスに関しては Open Shortest Path First（OSPF） 模造リンクおよび Multi Protocol Label Switching（MPLS）Virtual Private Networking（VPN）のために設定する必要があります。 この脆弱性は Supervisor Engine 32（Sup32）、Supervisor Engine 720（Sup720）または Route Switch Processor の Cisco Catalyst 6500 シリーズまたは Catalyst 7600 シリーズ デバイスだけに 720 の（RSP720）モジュール影響を与えます。 スーパバイザ 32、スーパバイザ 720、スーパバイザ 720-3B、スーパバイザ 720-3BXL、Route Switch Processor 720、Route Switch Processor 720-3C、および Route Switch Processor 720-3CXL は脆弱 なすべて可能性としてはです。

OSPF および MPLS VPNs はデフォルトで有効に なりません。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-queue で掲示されます。

注: 2008 年 3月 26 日パブリケーションは 5 つのセキュリティ アドバイザリが含まれています。 アドバイザリはすべて Cisco IOS に影響を与えます。 各アドバイザリはリリースをリストしアドバイザリに説明がある脆弱性を解決するアドバイザリはまたリリースをその正しいすべての 5 つのアドバイザリの脆弱性詳述します。

各ドキュメントへのリンクは次のとおりです。

- Cisco IOS バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）サービス拒否の脆弱性
  326-pptp

- Cisco IOS の多重 DLSw サービス拒否の脆弱性
  326-dlsw

- IPv4/IPv6 Dual-stack ルータのための Cisco IOS User Datagram Protocol（UDP）配信問題
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-IPv4IPv6

- OSPF、MPLS VPN およびスーパバイザ 32、スーパバイザ 720、または Route Switch Processor 720 の Cisco IOS の脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-queue

- Cisco IOS Multicast 仮想 な プライベート ネットワーク（MVPN）データ漏洩
  326-mvpn

該当製品

脆弱性のある製品

Supervisor Engine 32（Sup32）、Supervisor Engine 720（Sup720）、または Route Switch Processor 720（RSP720）に基づくすべてのシスコ製品は可能性としては脆弱です。 Cisco Sup720 および RSP720 製品に機能を高めるドータ カードのためのサポートがあります。 これらのドータ カードは Sup720 か RSP720 に直接接続し、PFC-3B、PFC-3BXL、PFC-3C および PFC-3CXL のような名前があります。 Sup720 または RSP720 の製品番号はインストールされている RSP720-3CXL のようなドータ カードを反映するために変更されることができます。

脆弱性が Sup720 および RSP720 に影響を与えるので、Sup720 のすべてのバージョンか RSP720 はインストールされているドータ カードに関係なく脆弱、です。

- Sup32、Sup720、Sup720-3B、または Sup720-3BXL の Cisco Catalyst 6500 シリーズ デバイス
- Sup32、Sup720、Sup720-3B、または Sup720-3BXL の Cisco 7600 シリーズ デバイス
- RSP720、RSP720-3C、または RSP720-3CXL の Cisco 7600 シリーズ デバイス
- Cisco ME 6524 イーサネット スイッチ

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

Cisco バグ ID CSCsf12082 （登録ユーザのみ）は脆弱 な ハードウェアで動作しない追加 IOS リリース、上でセクションがこの脆弱性から影響を受ける脆弱性が存在する製品で述べられたプラットフォームだけに統合されていましたが。

詳細

脆弱 な Ciscoデバイスは、Multi Protocol Label Switching （ MPLS ） Virtual Private Networking （ VPN ）および Open Shortest Path First (OSPF ）にせ物リンクのために設定されたとき、デバイスのブロックされたキュー、メモリリーク、および/または再始動で被害を受けることができます。

この脆弱性は Cisco バグ ID CSCsf12082 （登録ユーザのみ）で文書化されています、CVE ID CVE-2008-0537 を割り当てられました。

ハードウェア および ソフトウェア構成の次の組み合せは脆弱であるためにデバイスのためにある必要があります:

- Cisco Catalyst Sup32、Sup720、または RSP720 はあります
- MPLS VPN は設定されます
- OSPF にせ物リンクは設定されます

この機能を実行しているかどうか判別するために、**address-family vpnv4** および**エリアにせ物リンク** router configuration コマンドのために **show running-config コマンド**および検索を使用して下さい。 次のコマンドは次の条件を満たすすべての設定行を表示するものです:

- ワード「ルータから」、または始まります
- 「address-family がまたは vpnv4," 含まれています
- 含まれています「にせ物リンク」が

```
Router# show run | include ^router |address-family vpnv4|sham-link
router bgp 1
  address-family vpnv4
router ospf 1 vrf VRFNAME
 area 0 sham-link  192.168.1.1 192.168.100.1
Router#
```

セクション 修飾子をサポートする IOSバージョンを実行する顧客向けに、追加オプションは実行コンフィギュレーションの関連セクションを表示して利用できます:

```
Router# show run | section ^router
router bgp 1
[snip]
  address-family vpnv4
router ospf 1 vrf VRFNAME
 area 0 sham-link  192.168.1.1 192.168.100.1
[snip]
```

ある特定のパケットが上記の必要条件を満たすデバイスによって受信されれば、インターフェイスに入ることから追加トラフィックを禁止できるサービス拒否状態を引き起こし、これらのパケットをブロックされるようになることができる受信するインターフェイスのインプットキューにより。 潜在的なブロックされたインターフェイスキューに加えて、デバイスはまたメモリリークに苦しむか、または再起動できます。 メモリリークの場合に、デバイスは利用可能なメモリが減ればトラフィックを転送することができません。

MPLS VPNs に関する詳細については、次に挙げるドキュメントを参照して下さい:

http://www.cisco.com/en/US/docs/net_mgmt/vpn_solutions_center/1.1/user/guide/VPN_UG1.html

OSPF にせ物リンクに関する詳細については、次に挙げるドキュメントを参照して下さい:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ospfshmk.html

メモリリークの識別

この脆弱性は I/Oメモリ プールのリークとして明示できます。 以下は I/O プールの枯渇を示すシステムメッセージの例です:

```
006029: Aug  10: %SYS-2-MALLOCFAIL: Memory allocation of 808 bytes failed from 0x41613238,
alignment 32
Pool: I/O Free: 176  Cause: Not enough free memory
Alternate Pool: None  Free: 0  Cause: No Alternate pool
```

上記の出力の、影響を受けたメモリプールが**プール**であることに注目して下さい: **I/O** および原因は**原因**です: **ない十分 な 空き メモリ**。 この出力は I/Oメモリ プールが排出されたことを示したものです。

さらに、*イネーブル レベル* アクセスのユーザはバッファ割振り障害を識別する **show buffers コマンド**によってデバイスをチェックできます。

```
Router#show buffers
Buffer elements:
496 in free list (500 max allowed)
77298300 hits, 0 misses, 0 created

Public buffer pools:
Small buffers, 104 bytes (total 148654, permanent 1024, peak 148654 @ 1d12h):
0 in free list (128 min, 2048 max allowed)
24688031 hits, 4023203 misses, 0 trims, 147630 created
3243434 failures (3182828 no memory)
```

上記の出力はそのバッファ割り振りがメモリ不足が原因で失敗したことを示します。

ブロックされたインターフェイスの識別

ブロックされたキューのこの型の現象はきちんと影響を受けたインターフェイス上の接続を確立するルーティング プロトコル（OSPF、拡張内部ゲートウェイ ルーティング プロトコル（EIGRP）、ボーダー ゲートウェイ プロトコル（BGP）、Intermediate System to Intermediate System（ISIS）、等）および MPLS TDP/LDP のようなコントロール プレーン プロトコルの失敗です。

ブロックされたインプットインターフェイスを識別するために、インプットキュー ラインのための **show interfaces コマンド**および検索を発行して下さい。 インプットキューのサイズは増加し続けることができます。 下記の例の 76 である現在のサイズが大きければより最大サイズ（75）、インプットキューはブロックされます。

デバイスがコントロール プレーンに向かうトラフィックの高い率を受信するフルキューはただの一時イベントですことは可能性のあるであり。 インターフェイスが実際にブロックされるかどうか確認するために、**shutdown interface configuration コマンド**でインターフェイスをシャットダウンし、インプットキューを検査して下さい。 インプットキューが 0 パケットを表示する場合、インターフェイスはブロックされます。

```
Router#show interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is 0050.500e.f1e0 (bia 0050.500e.f1e0)
  Internet address is 172.16.1.9/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:41, output 00:00:07, output hang never
  Last clearing of "show interface" counters 00:07:18
  Input queue: 76/75/1091/0 (size/max/drops/flushes); Total output drops: 0

!--- The 76/75 shows that this is blocked
```

回避策

デバイス インターフェイスキューが排出されたら、デバイス 再始動だけがブロックされたキューの OSPF パケットをクリアできます。

これらのパケットが処理される方法が原因で、キュー ブロックは OSPF MD5 チェック前に発生します。 OSPF MD5 設定はこの脆弱性からデバイスを保護しません。

選択的パケット廃棄（SPD）Headroom の増加

最高で水平な基本はコントロール プレーン トラフィックに選択的パケット廃棄（SPD）拡張バッファリングを提供します。 SPD headroom として既知、この追加キュー項目数は 6（BGP のような）、コネクションレス型ネットワーク サービス（CLNS）によって基づくルーティング プロトコル Intermediate System-to-Intermediate System（IS-IS）、OSPF およびレイヤ2 キープアライブと等しい IP 優先順位でトラフィックのために一般的に予約済みです。

SPD headroom を増加することは OSPF パケットに追加バッファリングを提供します。 ブロッ

クされたキューの場合により多くのコントロール プレーン トラフィック バッファ領域を割り当てるために、SPD headroom は増加することができます。

SPD に関する詳細は次の白書で見つけることができます:

http://www.cisco.com/web/about/security/intelligence/spd.html

より多くのパケットを収容するためにキューサイズを拡張することは可能性のあるですが拡張されたキューが排出されるまでパケットはまだ集まることができます。 トラフィックがフローし続けるようにする一時的な次善策として入力待機キューは増やすことができます。 どの追加不正 なパケットでもまだキューを一杯にしますが、インプットキューが充満し、トラフィックがフローし終える前にインプットキュー深度を増加することは時間数を拡張できます。 次の例に 75 のデフォルトから最大 4096 に入力キューサイズを設定 する方法を示されています:

```
Router#show interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is 0050.500e.f1e0 (bia 0050.500e.f1e0)
  Internet address is 172.16.1.9/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:41, output 00:00:07, output hang never
  Last clearing of "show interface" counters 00:07:18
  Input queue: 76/75/1091/0 (size/max/drops/flushes); Total output drops: 0

!--- The 76/75 shows that this is blocked
```

OSPF 模造リンク 設定を取除くこと

脆弱性があることができるように OSPF 模造リンク 設定が必要となるので、模造リンク 機能を取除くことはこの脆弱性への公開を除去します。 OSPF 模造リンク 設定をデバイスから取除くために、OSPF 設定は模造リンクが設定される各インターフェイスで変更する必要があります。

OSPF 模造リンクの構成情報に関しては、次に挙げるドキュメントを参照して下さい:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ospfshmk.html

Cisco IOS Embedded Event Manager

Cisco IOS Embedded Event Manager (EEM) は Cisco IOSデバイスでイベント検出および反作用機能を提供します。 EEM ポリシーのブロックされたインターフェイスキューを検出する 可能性のあるです。 EEM は 管理者に対してインターフェースがブロックされたことを email, syslog メッセージ または Simple Network Management Protocol (SNMP) trap により警告することができます。

インターフェースがブロックされたことを管理者に syslog で警告することができるサンプル EEM ポリシーを EEM 専門のオンラインコミュニティ Cisco Beyond で入手することが出来ます

。 サンプル スクリプトは次のリンクで入手可能です:

http://forums.cisco.com/eforum/servlet/EEM?page=eem&fn=script&scriptId=981

EEM についての追加情報は、次の Cisco.com へのリンクより入手可能です:

http://www.cisco.com/en/US/products/ps6815/products_ios_protocol_group_home.html

修正済みソフトウェア

ソフトウェアのアップグレードを検討する際には、http://www.cisco.com/go/psirt およびそれ以降のアドバイザリも参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください

いずれの場合も、アップグレードする機器に十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。 情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Cisco IOS ソフトウェアの表（下掲）の各行には、Cisco IOS のリリース トレインが記載されています。 特定のリリース トレインに脆弱性がある場合は、修正を含む最初のリリース（および、それぞれの予想提供日）が表の「第 1 修正済みリリース」列に記載されます。 「推奨リリース」列には、このアドバイザリが作成された時点で発表されているすべての脆弱性の修正を含むリリースが記載されます。 特定の列に記されているリリースよりも古い（第 1 修正済みリリースより古い）トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。 表の「推奨リリース」列に記載されているリリース、またはそれよりも新しいリリースにアップグレードすることを推奨します。

メジャー リリース	**修正済みリリースの入手可能性**	
Affected 12.0-Based Releases	First Fixed Release（修正された最初のリリース）	**推奨リリース**
該当する 12.0 ベースのリリースはありません。		
Affected 12.1-Based Releases	First Fixed Release（修正された最初のリリース）	**推奨リリース**
該当する 12.1 ベースのリリースはありません。		
Affected 12.2-Based Release	First Fixed Release（修正された最初のリリース）	**推奨リリース**

s		
12.2	脆弱性なし	
12.2B	脆弱性なし	
12.2BC	脆弱性なし	
12.2BW	脆弱性なし	
12.2BY	脆弱性なし	
12.2BZ	脆弱性なし	
12.2CX	脆弱性なし	
12.2CY	脆弱性なし	
12.2CZ	脆弱性なし	
12.2DA	脆弱性なし	
12.2DD	脆弱性なし	
12.2DX	脆弱性なし	
12.2EU	脆弱性なし	
12.2EW	脆弱性なし	
12.2EWA	脆弱性なし	
12.2EX	脆弱性なし	
12.2EY	脆弱性なし	
12.2EZ	脆弱性なし	
12.2FX	脆弱性なし	
12.2FY	脆弱性なし	
12.2FZ	脆弱性なし	
12.2IXA	脆弱性あり; contact TAC	
12.2IXB	脆弱性あり; contact TAC	
12.2IXC	脆弱性あり; contact TAC	
12.2IXD	脆弱性あり; contact TAC	
12.2IXE	脆弱性あり; migrate to any release in 12.2IXF	12.2(18)IXF ; 31-MAR-2008 で利用可能
12.2JA	脆弱性なし	
12.2JK	脆弱性なし	
12.2MB	脆弱性なし	
12.2MC	脆弱性なし	
12.2S	脆弱性なし	
12.2SB	脆弱性なし	
12.2SBC	脆弱性なし	
12.2SCA	脆弱性なし	
12.2SE	脆弱性なし	
12.2SEA	脆弱性なし	
12.2SEB	脆弱性なし	
12.2SEC	脆弱性なし	
12.2SED	脆弱性なし	

12.2SEE	脆弱性なし	
12.2SEF	脆弱性なし	
12.2SEG	脆弱性なし	
12.2SG	脆弱性なし	
12.2SGA	脆弱性なし	
12.2SL	脆弱性なし	
12.2SM	脆弱性なし	
12.2SO	脆弱性なし	
12.2SRA	12.2(33)SRA4	12.2(33)SRA7
12.2SRB	脆弱性なし	
12.2SRC	脆弱性なし	
12.2SU	脆弱性なし	
12.2SV	脆弱性なし	
12.2SVA	脆弱性なし	
12.2SVC	脆弱性なし	
12.2SVD	脆弱性なし	
12.2SW	脆弱性なし	
12.2SX	脆弱性なし	
12.2SXA	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2SXB	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2SXD	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2SXE	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2SXF	12.2(18)SXF6	12.2(18)SXF13
12.2SXH	脆弱性なし	
12.2SY	脆弱性なし	
12.2SZ	脆弱性なし	
12.2T	脆弱性なし	
12.2TPC	脆弱性なし	
12.2UZ	脆弱性なし	
12.2XA	脆弱性なし	
12.2XB	脆弱性なし	
12.2XC	脆弱性なし	
12.2XD	脆弱性なし	
12.2XE	脆弱性なし	
12.2XF	脆弱性なし	
12.2XG	脆弱性なし	
12.2XH	脆弱性なし	
12.2XI	脆弱性なし	

12.2XJ	脆弱性なし	
12.2XK	脆弱性なし	
12.2XL	脆弱性なし	
12.2XM	脆弱性なし	
12.2XN	脆弱性なし	
12.2XO	脆弱性なし	
12.2XQ	脆弱性なし	
12.2XR	脆弱性なし	
12.2XS	脆弱性なし	
12.2XT	脆弱性なし	
12.2XU	脆弱性なし	
12.2XV	脆弱性なし	
12.2XW	脆弱性なし	
12.2YA	脆弱性なし	
12.2YB	脆弱性なし	
12.2YC	脆弱性なし	
12.2YD	脆弱性なし	
12.2YE	脆弱性なし	
12.2YF	脆弱性なし	
12.2YG	脆弱性なし	
12.2YH	脆弱性なし	
12.2YJ	脆弱性なし	
12.2YK	脆弱性なし	
12.2YL	脆弱性なし	
12.2YM	脆弱性なし	
12.2YN	脆弱性なし	
12.2YO	脆弱性なし	
12.2YP	脆弱性なし	
12.2YQ	脆弱性なし	
12.2YR	脆弱性なし	
12.2YS	脆弱性なし	
12.2YT	脆弱性なし	
12.2YU	脆弱性なし	
12.2YV	脆弱性なし	
12.2YW	脆弱性なし	
12.2YX	脆弱性なし	
12.2YY	脆弱性なし	
12.2YZ	脆弱性なし	
12.2ZA	脆弱性なし	
12.2ZB	脆弱性なし	
12.2ZC	脆弱性なし	
12.2ZD	脆弱性なし	

12.2ZE	脆弱性なし	
12.2ZF	脆弱性なし	
12.2ZG	脆弱性なし	
12.2ZH	脆弱性なし	
12.2ZJ	脆弱性なし	
12.2ZL	脆弱性なし	
12.2ZP	脆弱性なし	
12.2ZU	脆弱性あり; migrate to any release in 12.2SXH	12.2(33)SXH2
12.2ZY	脆弱性なし	
Affected 12.3-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
該当する 12.3 ベースのリリースはありません。		
Affected 12.4-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
該当する 12.4 ベースのリリースはありません。		

不正利用事例と公式発表

Cisco PSIRT はこのアドバイザリに記載される脆弱性の公示か不正利用に気づいていません。

この脆弱性は、お客様 によって Cisco に報告されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-queue

改訂履歴

リビジョン 1.3	2008-June-27	リンクおよび冗漫を取除く更新済要約。
リビジョン 1.2	2008-April-25	CSCsf12082 への更新済 CVSS リンク。
リビジョ	2008-March-	要約するとセクションは IPv4/IPv6 Dual-stack ルータのための Cisco IOS 配信問

ン 1.1	26	題に、テキスト User Datagram Protocol (UDP) 変更し、詳細 セクションで、テキストは CVE-2008-0537 に変更しました。
リビジョン 1.0	2008-March-26	初回公開リリース

利用規約

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。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。