Cisco Security Notice： W32.BLASTER ワームの影響を軽減するための推奨事項

目次

要約
詳細情報
検出方法
 IOS の NetFlow を有効にして感染したホストを検出する
 Sup2 を搭載した CatOS および MLS を使用して感染したホストを検出する
 CSIDS のシグニチャ
症状
該当製品
ソフトウェアのバージョンおよび修正
 Cisco Secure ACS Solution Engine/Cisco Secure ACS Appliance
 Cisco CallManager、Cisco Customer Response Server/Cisco IP Contact Center Express、Cisco Personal Assistant、Cisco Conference Connection、Cisco Emergency Responder
 Cisco Building Broadband Service Manager
 その他の Windows ベースのシスコ製品
修正済みソフトウェアを入手する
回避策
 IOS 用 ACL
 Cisco 12000
 6500 上の VACL
 Catalyst 3550
 Catalyst 2950
 Catalyst 2900XL および 3500XL
 PIX
DoS 攻撃の軽減方法
不正利用および公表
この通知のステータス： 暫定版
配信
改訂履歴
シスコのセキュリティ手順
関連情報

要約

現在、インターネット上に広がっている新しいワームによる攻撃が発生しています。 このワームの現象として、ポート 69 に対する UDP トラフィックおよびポート 135 と 4444 に対する大量の TCP トラフィックが発生します。このワームの影響を受けたお客様には、内部システムと外部システムの両方から、大量のトラフィックが生じています。 シスコ製デバイス上の症状としては、CPU 使用率の上昇および入力インターフェイスでのトラフィックの廃棄が見られますが、他の症状が起こる可能性もあります。 この文書では、症状の軽減方法および該当するシスコ製品を説明します。これらの製品には、シスコからのソフトウェア パッチを適用する必要があります。

このワームは、「W32.Blaster」、「msblast.exe」、「Lovsan」、「Poza」、「Exploit-DcomRpc」と呼ばれています。 このワームは、Microsoft が以前に開示した脆弱性を不正に利用しています。詳細については、次の URL を参照してください。

http://www.microsoft.com/technet/security/bulletin/MS03-026.asp

MS03-026 のパッチが適用されていないシステムを不正利用するワームは、現在 2 種類あり、それぞれ Blaster および Nachi と呼ばれています。 この文書では、Blaster の症状を軽減する方法を説明します。Nachi の症状を軽減する方法は、http://www.cisco.com/japanese/warp/public/3/jp/service/tac/707/cisco-sn-20030820-nachi-j.shtml にある別の文書で説明します。 これらの問題に軽減方法を実行する際には、両方の文書を検討してください。

詳細情報

このワームの詳細情報は Microsoft の次の Web サイトに説明されています。

http://www.microsoft.com/technet/security/virus/alerts/msblaster.asp

このワームの影響は、ワームの感染、さらなる感染先のスキャン、および実行形式コードの伝播に必要とされるポートをブロックすることで軽減できます。 この文書では、内部ネットワークが感染する前または後に、ワームの感染が広がるのを防ぐ方法を中心に説明します。 このワームは通常使用されるポートを使用して広がるので、これらのポートをブロックすると、ファイル共有、TFTP、Kerberos 認証などの既存の機能が動作しなくなる可能性があります。 すべてのネットワーク設定と同様に、シスコでは、通常時のベースライン トラフィックを文書化し、その情報に基づいて、ネットワークのポートまたはトラフィックをブロックするかどうかを判断することをお勧めします。 ネットワークの機能を損なわないように、ポートのブロックは慎重に行ってください。 以下に、これらのポートの一般的な用途を簡単に列挙します。

TCP ポート 135 は MS RPC プロトコル用に使用されます。 このプロトコルは、複数のローカル ネットワーク セグメント間のファイルの共有に使用されますが、まれに複数の WAN セグメント間のファイルの共有に使用される場合もあります。 まず、このポートから脆弱性が不正使用され、コンピュータを完全に感染させるための一連のイベントが開始されます。 ポート 135 をブロックすると最初の感染は防止できますが、ネットワーク内の既存のファイル共有機能が使用できなくなる可能性があります。

UDP ポート 69 は、Trivial File Transport Protocol（TFTP）用に使用されており、新しいソフトウェア イメージまたは設定をネットワークに接続されたデバイスにロードするためによく使用されます。 W32.Blaster ワームに感染したホストは、このポートを開放して、すでに感染したコンピュータから新しく不正使用するコンピュータに msblast.exe ファイルを転送します。 このポートをブロックすると、すでに感染したコンピュータから脆弱性のあるコンピュータにワームが広がるのを防止できる可能性がありますが、Voice over IP の一部の実装にも利用されている、ネットワーク内の既存の TFTP 機能が使用できなくなる可能性があります。

TCP ポート 4444 は Kerberos 認証および Oracle9i の通信に使用されています。 W32.Blaster ワームに完全に感染したホストは、このポート上にリモートコマンドシェル用のポートをオープンし、コンピュータをリモートから制御可能にします。 このポートをブロックすると、感染したコンピュータがさらに悪意のある活動に使用されるのを防止できる可能性がありますが、ネットワーク内の既存の Kerberos 認証機能または Oracle9i の実装が使用できなくなる可能性があります。

TCP および UDP の両方、あるいはその一方のポート 137、138、139、593 には、これに関連した脆弱性があり、ホストが不正使用される危険にさらされる可能性があります。ただし、現時点ではこれらが W32.Blaster ワームの感染拡大に直接関係しているとは考えられていません。 シスコでは、不必要なすべてのポート、特に既知の脆弱性があることが判明しているポートの送受信をネットワーク エッジでブロックして、リモートからの不正使用を防ぐことをお勧めします。

検出方法

IOS の NetFlow を有効にして感染したホストを検出する

NetFlow は、感染したホストを特定する強力なツールとして使用できます。 インターフェイス上で ip route-cache flow コマンドを使用して、Netflow を有効にしてください。 次の例では、感染したホストが宛先ポート 135（出力上の表示は 0087）経由で任意のシステムに感染を試みています。ポート 69 は 0045、ポート 4444 は 115c と表示されています。

```
Router>show ip cache flow | include 0087

    SrcIf      SrcIPaddress    DstIf    DstIPaddress  Pr SrcP DstP    Pkts

    Fa2/0      XX.XX.XX.242    Fa1/0    XX.XX.XX.119  06 0B88 0087    1

    Fa2/0      XX.XX.XX.242    Fa1/0    XX.XX.XX.169  06 0BF8 0087    1

    Fa2/0      XX.XX.XX.204    Fa1/0    XX.XX.XX.63   06 0E80 0087    1

    Fa2/0      XX.XX.XX.204    Fa1/0    XX.XX.XX.111  06 0CB0 0087    1

    Fa2/0      XX.XX.XX.204    Fa1/0    XX.XX.XX.95   06 0CA0 0087    1

    Fa2/0      XX.XX.XX.204    Fa1/0    XX.XX.XX.79   06 0C90 0087    1
```

Sup2 を搭載した CatOS および MLS を使用して感染したホストを検出する

MLS の統計情報は、感染したホストの追跡に役立ちます。 次の例のように、NetFlow を full flow モードにして、送信元ポートと宛先ポートを表示してください。この例では、感染したホストからトラフィックが発信され、宛先ポート TCP 135 経由で任意のシステムに感染を試みています。

```
Router>(enable)set mls flow full

    Router>show mls statistics entry ip dst-port 135

                                    Last    Used

    Destination IP   Source IP       Prot  DstPrt SrcPrt Stat-Pkts  Stat-Bytes

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

XX.XX.XX.28	XX.XX.XX.10	TCP	135	2329	0	0
XX.XX.XX.58	XX.XX.XX.28	TCP	135	2342	0	0
XX.XX.XX.141	XX.XX.XX.223	TCP	135	2333	0	0
XX.XX.XX.189	XX.XX.XX.1	TCP	135	2347	0	0
XX.XX.XX.12	XX.XX.XX.19	TCP	135	2328	0	0
XX.XX.XX.245	XX.XX.XX.137	TCP	135	2343	0	0
XX.XX.XX.29	XX.XX.XX.22	TCP	135	2318	0	0

CSIDS のシグニチャ

Cisco Secure Intrusion Detection System（IDS; 侵入検知システム）を使用している場合、シグニチャの更新ファイルが次の場所にあります。 http://www.cisco.com/support/ja/707/idsfaq.shtml（登録ユーザのみ）

S49 に対する False Positive（誤検知）を減らすために、シグニチャ 3327 を設定して、ポート 139 および 445 ではなく、ポート 135 だけを検査する必要があります。

または、このワームに対処するためのカスタム シグニチャ文字列を追加する方法もあります。 以下に、その方法を簡単に説明します。

```
Engine STRING.UDP

    SigName MS Blast Worm TFTP Request

    ServicePorts 69

    RegexString ¥x00¥x01[Mm][Ss][Bb][Ll][Aa][Ss][Tt][.][Ee][Xx][Ee]¥x00

    Direction ToService
```

症状

感染した Microsoft ホストの症状については、http://www.microsoft.com/technet/security/virus/alerts/msblaster.asp にある Microsoft の速報を参照してください。

ネットワーク全体の症状としては、トラフィックの増大により、ファイアウォール、ルータ、スイッチの負荷が高まる場合があります。 負荷が高まるため、ネットワークが不安定になる場合もあります。 このワームが原因でトラフィックに高い負荷が発生しますが、感染後、最初の 24 時間を過ぎると安定する傾向にあります。

通常使用されるポートをフィルタ対象とする場合、正当なサービスがフィルタリングされたりブロックされたりするため、予想外のネットワーク障害が発生する場合があります。たとえば、ルータ、IP フォンなどがブートしない場合、これらのデバイスから TFTP サーバにアクセス可能かどうかを確認してください。 これらのデバイスは、W32.Blaster ワームに対して脆弱ではありませんが、ブート時にソフトウェアまたは設定ファイルをロードするために、TFTP の機能を利用している場合があります。

該当製品

製品に脆弱性があるかどうかについては、以下のリストを確認してください。 ソフトウェア バージョンまたは設定情報が示されている場合は、その組み合せにのみ脆弱性があります。 このリストに示されている装置用ソフトウェアには、パッチをシスコからダウンロードして適用する必要があります。

- Cisco Secure ACS Solution Engine（別名 Cisco Secure ACS Appliance）
- Cisco CallManager
- Cisco Building Broadband Service Manager（BBSM）
    - BBSM バージョン 5.1
    - BBSM バージョン 5.2
    - HotSpot 1.0
- Cisco Customer Response Application Server（CRA）
- Cisco Personal Assistant

- Cisco Conference Connection（CCC）
- Cisco Emergency Responder

Microsoft のオペレーティング システム上で動作するその他のシスコ製品については、次の Microsoft のパッチを適用することを強くお勧めします。

http://www.microsoft.com/technet/security/bulletin/MS03-026.asp

このリストにすべてが網羅されているとは限りません。該当する Microsoft のプラットフォームを使用していると考えられる場合は、Microsoft の速報を参照してください。

- Cisco Unity
- Cisco uOne Enterprise Edition
- Cisco Network Registrar（CNR）
- Cisco Internet Service Node（ISN）
- Cisco Intelligent Contact Manager（ICM）（Hosted および Enterprise）
- Cisco IP Contact Center（IPCC）（Express および Enterprise）
- Cisco E-mail Manager（CEM）
- Cisco Collaboration Server（CCS）
- Cisco Dynamic Content Adapter（DCA）
- Cisco Media Blender（CMB）
- TrailHead（Web Gateway ソリューションの一部）
- Cisco Networking Services for Active Directory（CNS/AD）
- Cisco SN 5400 シリーズ ストレージ ルータ（Windows サーバへのインターフェイスとなるドライバ）
- CiscoWorks
    - CiscoWorks VPN/Security Management Solution（CWVMS）
    - User Registration Tool
    - LAN Management Solution
    - Routed WAN Management
    - Service Management
    - VPN/Security Management Solution
    - IP Telephony Environment Monitor
    - Small Network Management Solution
    - QoS Policy Manager
    - Voice Manager
- Cisco Transport Manager（CTM）
- Cisco Broadband Troubleshooter（CBT）
- DOCSIS CPE Configurator
- Cisco Secure アプリケーション
    - Cisco Secure Scanner

- Cisco Secure Policy Manager（CSPM）
- Access Control Server（ACS）

- テレビ会議用アプリケーション
  - IP/VC 3540 Video Rate Matching Module
  - IP/VC 3540 Application Server

ソフトウェアのバージョンおよび修正

Cisco Secure ACS Solution Engine/Cisco Secure ACS Appliance

ソフトウェア バージョン 3.2.1 が影響を受けます。 CiscoSecure ACS Solution Engine Hotfix KB824146 バージョン 3.2（1.20）では、Microsoft のパッチ MS03-026 に取って代わる MS03-039 を適用し、TCP/UDP 137、138、445 の各ポートを無効にすることによって基盤となるオペレーティング システムに他のセキュリティ対策を追加することで、この脆弱性を解決しています。

このファイルは、http://www.cisco.com/pcgi-bin/tablebuild.pl/solution_engine からダウンロードできます。

ソフトウェア リリース 3.2.2 以上には、このパッチが含まれます。

どのバージョンがインストールされており、Cisco Secure ACS Solution Engine にホットフィックスまたはパッチが存在するかを確認するには、System Configuration メニューをチェックしてから、Appliance Upgrade Status 項目を選択します。

アップグレード手順またはホットフィックスを CiscoSecure ACS Solution Engine に適用する手順は、http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacsapp/install/admap.htm#1044616 に記載されています。これは、ホットフィックス ファイルに付随する Readme.txt ファイルに含まれています。

この手順の詳細については、マニュアルを参照するか、Technical Assistance Center までご連絡ください。

Cisco CallManager、Cisco Customer Response Server/Cisco IP Contact Center Express、Cisco Personal Assistant、Cisco Conference Connection、Cisco Emergency Responder

オペレーティング システムのバージョンが Win2000 2.4 である場合、次のいずれかをダウンロードしてインストールする必要があります。

- 最新のサービス パック： win-OS-Upgrade-k9.2000-2-4sr5.exe
- この問題に対するホットフィックス： win-K9-MS03-026.exe

いずれも http://www.cisco.com/pcgi-bin/tablebuild.pl/cmva-3des から入手できます。

Cisco Building Broadband Service Manager

BBSM 5.1、5.2、および HotSpot 1.0 にパッチを適用するためのソフトウェアが、シスコの Web サイトにあります。

- Cisco BBSM 5.2：RPCBufferOverrun.exe を http://www.cisco.com/pcgi-bin/tablebuild.pl/bbsm52 からダウンロードします（登録ユーザのみ）
- Cisco BBSM 5.1：RPCBufferOverrun.exe を http://www.cisco.com/pcgi-bin/tablebuild.pl/bbsm51 からダウンロードします（登録ユーザのみ）
- Cisco BBSM HotSpot1.0：RPCBufferOverrun.exe を http://www.cisco.com/pcgi-bin/tablebuild.pl/bbsmhs10 からダウンロードします（登録ユーザのみ）

BBSM にサービス パッチをインストールする方法については、次のサイトを参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm52/user/use52_05.htm#50416

その他の Windows ベースのシスコ製品

次に示す Microsoft のサイトから直接セキュリティ パッチをダウンロードして、インストールの指示に従ってください。
http://www.microsoft.com/technet/security/bulletin/MS03-026.asp

修正済みソフトウェアを入手する

シスコが製品にオペレーティング システムを組み込んで提供している場合は、該当するお客様すべてに対して、これらの脆弱性に対処するためのソフトウェアのパッチをシスコが無料で提供しています。 お客様がインストールしたり、サポートを受けたりできるのは、ご購入いただいた機能セットに対してのみです。

サービス契約をご利用いただいている場合、通常のアップデート窓口に連絡して、ご購入いただいた機能セットを含むソフトウェア パッチを入手してください。 サービス契約をご利用いただいている場合は、通常、http://www.cisco.com/tacpage/sw-center/ にあるシスコのワールドワイド ウェブの Software Center からパッチを入手してください。

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡して、無料のソフトウェア パッチを入手してください。

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、以下の連絡先リストにあるシスコの Technical Assistance Center（TAC）に連絡して修正済みソフトウェアを入手してください。 この場合、同じリリースの新しいバージョンに対するパッチ、またはソフトウェアのバージョンおよび修正の表（前述）の該当する行に示されているパッチを入手できます。

Cisco TAC の連絡先は以下のとおりです。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール： tac@cisco.com

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、http://www.cisco.com/cisco/web/support/JP/cisco_worldwide_contacts.html を参照してください。

注：弊社とのサポート契約がないお客様は、製品をご購入いただきました販売店経由でお問い合わせください。

無料アップグレードの対象であることをご証明いただくために、製品のシリアル番号を用意し、この通知の URL をお知らせください。

ソフトウェアのアップグレードについては、「psirt@cisco.com」または「security-alert@cisco.com」には連絡しないでください。

回避策

このセクションでは、ネットワーク上の既存のシスコ製品を使用して、W32.Blaster ワームの症状を軽減する方法を説明します。これらの手法は、既存のネットワークの機能に影響を与えないと判断できた場合に、ネットワーク エッジでの送受信に適用してください。 この後も、感染しているシステムは感染したままで、ネットワークのそのセクション内では感染を拡大させます。このため、Microsoft の勧告に従って、感染しているシステムすべてにパッチを適用することをお勧めします。

これらの例はそれぞれ、該当するすべてのポートをブロックする方法を示していますが、該当するすべてのポートをブロックする必要がない場合もあります。 ネットワーク内に感染したホストがない場合、ネットワーク エッジのポート 135 をブロックするだけで十分な場合もあります。これにより、既存の TFTP および Kerberos のサービスを妨げることなく、ネットワークの外部からの感染を防止できます。 ネットワークの通常のトラフィック フローを NetFlow を使用して識別すれば、これらの軽減方法を適用する際にその影響を最小限に抑えることができます。

分散サービス拒絶攻撃からの保護方法に関する一般情報については、http://www.cisco.com/japanese/warp/public/3/jp/service/tac/707/newsflash-j.html を参照してください。

注意：すべての設定変更と同様に、この設定の影響を十分に検討してから変更を適用してください。

IOS 用 ACL

以下に特に明記されていない限り、この回避策はほとんどのルータ プラットフォームに適用できます。

注：送信元アドレスを追跡する場合、ACL の log 文ではなく Sampled NetFlow を使用してください。「log」文を高トラフィック時に使用すると、ルータが処理しきれなくなる可能性があります。

```
! --- TFTP をブロック

access-list 115 deny udp any any eq 69

! --- W32.Blaster に関連するプロトコルをブロック

access-list 115 deny tcp any any eq 135
access-list 115 deny udp any any eq 135

! --- 脆弱性のあるその他の MS プロトコルをブロック

access-list 115 deny udp any any eq 137
access-list 115 deny udp any any eq 138
access-list 115 deny tcp any any eq 139
access-list 115 deny udp any any eq 139
access-list 115 deny tcp any any eq 445
access-list 115 deny tcp any any eq 593

! --- W32.Blaster によるリモート アクセスをブロック

access-list 115 deny tcp any any eq 4444

! --- その他のトラフィックはすべて許可 -- その他の
! --- 既存のアクセスリスト エントリをここに挿入

access-list 115 permit ip any any
interface <interface>
ip access-group 115 in
ip access-group 115 out
```

このワームは任意の IP アドレスにパケットを送信しようとするので、その IP アドレスが存在しない場合もあります。 この場合、ルータは「ICMP unreachable」パケットを応答します。 不正な IP アドレスに対する大量の要求に応答するため、ルータのパフォーマンスが低下する場合があります。 これを防ぐには、次のコマンドを使用します。

```
Router(config)# interface <interface>
    Router(if-config)# no ip unreachables
```

注意：特定ののトンネル構造など、一般的なネットワーク設定に「ip unreachables」を使用する必要があります。 「ICMP unreachable」パケットをルータが送信可能にしておく必要がある場合は、次のコマンドを使用して時間当たりの応答回数を制限できます。

```
Router(config)# ip icmp rate-limit unreachable <millisecond>
```

Cisco IOS ソフトウェア リリース 12.0 以降では、デフォルトの制限は、1 秒当たり 2 パケット（500 ミリ秒）です。一般に使用される値は 2000 ミリ秒です。

Cisco 12000

受信 ACL 機能：Cisco 12000（GSR）シリーズ ルータでは、ルータ自体の IP アドレスを宛先とするパケットは、Gigabit Route Processor（GRP; ギガビット ルート プロセッサ）に処理が任されます。 GRP を保護するために、受信 ACL（rACL）を適用できます。rACL では、GRP 宛てのトラフィックをフィルタして、明示的に許可されたトラフィックだけを GRP で処理し、拒否されたトラフィックを廃棄します。 一般に、rACL は通過トラフィック（ルータを通過するトラフィック）には影響せず、ルータ自体を宛先とするトラフィックのみに影響します。

rACL は、GRP 宛ての過度の攻撃トラフィックの影響を軽減するのに非常に効果的な対抗手段です。 詳細については、次を参照してください。 GSR: 受信アクセス コントロール リスト（rACL）.

6500 上の VACL

シスコでは、Sup3 を搭載した Cisco Catalyst 4000 およびハイブリッドまたはネイティブ構成の Cisco Catalyst 6500 で IOS ACL を使用することをお勧めします。ただし、参考として、VACL の設定例を示します。 さらに、「no ip unreachables」を使用することもお勧めします。

注意：すべての設定変更と同様に、VACL を IOS ACL と併用する場合は注意してください。 VACL は方向にかかわらず、VLAN 内のすべてのトラフィックに適用されることに注意してください。

設定するには次の操作をします。

```
! --- TFTP をブロック

set security acl ip BLASTER deny udp any any eq 69

! --- 脆弱性のある MS プロトコルをブロック
! --- Blaster に関連のあるもの

set security acl ip BLASTER deny tcp any any eq 135
set security acl ip BLASTER deny udp any any eq 135

! --- Blaster に関連のないもの

set security acl ip BLASTER deny tcp any any eq 137
set security acl ip BLASTER deny udp any any eq 137
set security acl ip BLASTER deny tcp any any eq 138
set security acl ip BLASTER deny udp any any eq 138
set security acl ip BLASTER deny tcp any any eq 139
set security acl ip BLASTER deny udp any any eq 139
set security acl ip BLASTER deny tcp any any eq 593

! --- W32.Blaster によるリモート アクセスをブロック

set security acl ip BLASTER deny tcp any any eq 4444
```

```
! --- その他のトラフィックはすべて許可

! --- その他の既存のアクセスリスト エントリをここに挿入


set security acl ip BLASTER permit any any


! -- 受信側と送信側の両方に適用


commit security acl BLASTER

set security acl map BLASTER <vlans>
```

確認するには次の操作をします。

```
show security acl info all
```

削除するには次の操作をします。

```
clear security acl BLASTER

commit security acl BLASTER
```

Catalyst 3550

VLAN に対するレイヤ 3 インターフェイスである Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）、物理レイヤ 3 インターフェイス、およびレイヤ 3 イーサネット インターフェイスの送受信両方、あるいは一方に IOS ACL を適用します。 インターフェイスに「no ip unreachable」が設定されていることを確認してください。

IOS ACL がレイヤ 3 インターフェイスの入力側にも適用されていない場合にのみ、IOS ACL をスイッチのレイヤ 2 インターフェイスに適用します（このとき、エラーメッセージが発行されます）。 レイヤ 2 インターフェイスについては、IOS ACL がサポートされるのは物理インターフェイスのみで、EtherChannel インターフェイスではサポートされません。 また、適用できるのは受信方向のみです。

Catalyst 2950

IOS ACL をインターフェイスに適用します。 ACL がサポートされるのは受信方向のみであることに注意してください。 ACL を物理インターフェイスに適用するには、拡張ソフトウェア イメージ（EI）をインストールする必要があります。

Catalyst 2900XL および 3500XL

これらのレイヤ 2 スイッチでは、レイヤ 3 アクセス リストがサポートされません。

PIX

PIX のデフォルトの動作では、該当するポートおよびプロトコルに対してアクセスリストまたはコンジットによる明示的な許可がない場合は、下位のセキュリティ レベル インターフェイス（OUTSIDE）から上位のセキュリティ レベル インターフェイス（INSIDE）へのトラフィックをブロックします。

さらに、シスコでは、上位のセキュリティ レベル インターフェイス（INSIDE）から下位のセキュリティ レベル インターフェイス（OUTSIDE）へのトラフィックをブロックすることも推奨しています。

次のポートに対する発信要求を拒否する必要があります。

```
access-list acl_inside deny udp any any eq 69

access-list acl_inside deny tcp any any eq 135

access-list acl_inside deny udp any any eq 135
```

```
access-list acl_inside deny tcp any any eq 137

access-list acl_inside deny udp any any eq 137

access-list acl_inside deny tcp any any eq 138

access-list acl_inside deny udp any any eq 138

access-list acl_inside deny tcp any any eq 139

access-list acl_inside deny udp any any eq 139

access-list acl_inside deny tcp any any eq 445

access-list acl_inside deny tcp any any eq 593

access-list acl_inside deny tcp any any eq 4444


! --- 以前に設定した ACL 文をここに挿入、あるいは、

! --- その他の送信トラフィックをすべて許可


access-list acl_inside permit ip any any




access-group acl_inside in interface inside
```

対応する発信リストを適用することもできますが、発信リストの代わりに ACL を使用することを強くお勧めします。

DoS 攻撃の軽減方法

W32.Blaster ワームは、まず 2003 年 8 月 16 日に windowsupdate.com に対して TCP SYN 攻撃を開始するように設定されています。

感染したホストが生成するパケットは、windowsupdate.com のホスト名で解決された IP アドレスの http ポート（TCP/80）を宛先としています。送信元アドレスは、感染したホストと同じ B クラスの任意のアドレスにスプーフィング（偽装）されています。 そのため、アンチスプーフィング手法を実施すれば、DoS 攻撃の影響を軽減する上で役立つ場合があります。

シスコ製ルータには、Unicast Reverse Path Forwarding（ユニキャスト RPF）とアクセスリストの一般的な 2 種類のアンチスプーフィング手法があります。

ユニキャスト RPF がインターフェイスで有効にされると、ルータはそのインターフェイスで受信したすべてのパケットを検査して、送信元アドレスと送信元インターフェイスが、パケットを受信したインターフェイスと一致していることを確認し、そうでない場合はパケットが廃棄されます。 ユニキャスト RPF の詳細については、「ユニキャスト Reverse Path Forwarding (RPF)の設定」を参照してください。

アンチスプーフィング用アクセスリストを実装するには、特定のインターフェイスに正当な送信元アドレスとして表示される可能性、そのネットワークに対する明確な知識が必要です。 ip access-group <acl> in コマンドを使用して、承認されたすべてのネットワークのアクセスを許可し、他の IP アドレス空間を拒否するアクセスリストをインターフェイスに設定すれば、スプーフィングされたパケットをインターフェイス上で廃棄できます。

たとえば、fastethernet0/0 経由で 192.168.1.0/24 の内部ネットワークに接続された企業ルータ上で、内部ネットワークから送信されるスプーフィングされたパケットを廃棄するには、次のアクセスリストを使用できます。

```
access-list <access-list> permit 192.168.1.0 0.0.0.255

access-list <access-list> deny any

interface fastethernet 0/0

  ip access-group <access-list> in
```

上の例の <access-list> は、1 99 または 1300 1999（IP 標準アクセスリストの範囲）の未使用のアクセスリスト番号である必要があります。

アンチスプーフィングの手法としては、可能な限り、アクセスリストではなくユニキャスト RPF を使用することをお勧めします。

アンチスプーフィングの詳細については、「Cisco ルータにおけるセキュリティの向上」のアンチスプーフィングのセクションを参照してください。

不正利用および公表

この問題の不正利用は頻繁に行われており、多くの発表やメッセージが公表されています。 次のような参考資料があります。

- http://www.eeye.com/html/Research/Advisories/AL20030811.html
- http://www.cert.org/advisories/CA-2003-20.html

この通知のステータス： 暫定版

この通知は暫定通知です。 シスコは、この通知のすべての内容が正確であることを保証しませんが、可能な限りすべての事実を確認しています。 シスコは、これらの事実に重大な変更があれば、この通知のアップデート バージョンを発行する予定です。

配信

この通知はシスコのワールドワイド ウェブサイトの http://www.cisco.com/cisco/web/support/JP/100/1006/1006458_cisco-sn-20030814-blaster-j.html に公開されます。 ワールドワイド ウェブへの掲載に加えて、この通知のテキスト バージョンが、シスコの PSIRT PGP キーによるクリア署名付きで、以下の電子メールおよび Usenet ニュースの受信者に公開されます。

- cust-security-announce@cisco.com

将来、この通知がアップデートされた場合、シスコのワールドワイド ウェブに掲載されます。 この問題に関心のある方は、上記の URL でアップデートを確認することをお勧めします。

改訂履歴

リビジョン 1.0	2003 年 8 月 14 日	初期公開
リビジョン 1.1	2003 年 8 月 15 日	DoS 攻撃の軽減方法に関するセクションを追加
リビジョン 1.2	2003 年 8 月 16 日	該当製品リストにテレビ会議製品を追加、 VoIP の一部の実装方法がポート 69 のブロックで受ける可能性のある影響を明記、 CRS（IPCC Express）の新しい名前を明確化のために追加。
リビジョン 1.3	2003 年 8 月 18 日	CATOS の例を正しいコマンド構文にアップデート。
リビジョン 1.4	2003 年 8 月 18 日	ポート 4444 の 16 進数への変換を訂正。
リビジョン 1.5	2003 年 8 月 21 日	要約セクションの終わりに Nachi ワームについての段落を追加。
リビジョン 1.6	2003 年 10 月 14 日	該当製品およびソフトウェアのバージョンおよび修正の各セクションに Cisco Secure ACS Solution Engine を追加。
リビジョン 1.7	2003 年 12 月 9 日	Wireless LAN Solution Engine は脆弱でないため、該当製品セクションから削除。

シスコのセキュリティ手順

有益な新情報をお持ちの場合、psirt@cisco.com まで電子メールでご連絡ください。

シスコ製品のセキュリティの脆弱性に関するレポート、セキュリティ障害に対する支援、およびシスコからのセキュリティ情報を

受信するための登録に関するすべての情報は、シスコのワールドワイド ウェブサイト http://www.cisco.com/japanese/warp/public/3/jp/service/tac/707/sec_incident_response-j.html から入手できます。 この情報には、シスコのセキュリティ通知に関して、報道機関が問い合せる場合の説明も含まれています。 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。

Updated: 2004 年 1 月 27 日 Document ID: 44522

http://www.cisco.com/cisco/web/support/JP/100/1006/1006458_cisco-sn-20030814-blaster-j.html