MS06-040サービスバッファの脆弱性の悪用に対する緩和策

アドバイザリーID : cisco-sa-20060814-ms06-040-vulnerability
初公開日 : 2000-08-14 23:00
バージョン 1.1 : Final
回避策 : No Workarounds available
Cisco バグ ID :

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

脆弱性の特性

この脆弱性は、認証やユーザの操作なしで、リモートから悪用される可能性があります。不正利用されると、攻撃者はシステムの特権でリモートコード実行を実行したり、サービス拒否(DoS)を引き起こしたりする可能性があります。この攻撃方法は、TCP ポート 139 および 445 を介するものです。この脆弱性は、CVE ID 2006-3439で指定されています。

脆弱性の概要

このドキュメントには、Microsoft Serverサービスのバッファオーバーフローの脆弱性を不正利用する試みを緩和するためにCiscoのお客様を支援する情報が含まれています。Server Serviceにはリモートコード実行の脆弱性があり、攻撃者がこの脆弱性の悪用に成功すると、影響を受けるシステムを完全に制御できるようになる可能性があります。

次のオペレーティングシステムを使用しているコンピュータが該当します。

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1
- Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 Service Pack 1
- Itaniumベースのシステム用のMicrosoft Windows Server 2003
- Itaniumベースシステム用Microsoft Windows Server 2003 SP1
- Microsoft Windows Server 2003 x64 Edition

該当するWindowsプラットフォームの詳細については、MS06-040を参照してください。

緩和テクニックの概要

Ciscoデバイスには、MS06-040の脆弱性に対する複数の対応策があります。最も防止的な制御は、Cisco Security Agent(CSA)によってエンドホストレベルで提供されます。CSAのデフォルトの有効ルールセットは、すべての既知の攻撃ベクトルからの脅威を軽減します。Cisco IPS製品スイートでは、シグニチャ5799/0-

5799/7を使用するシグニチャパックS243から検出制御を実行できます。Cisco IOS®ソフトウェア、PIX、およびASAに適用されたアクセスリストと、VPN接続に適用されたアクセスコントロールにより、抑止が提供され、脅威にさらされる可能性が低減されます。

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。該当する製品とリリースは多岐に渡るので、サービス プロバイダーやサポート機関に連絡し、ネットワーク内で使用するのに最も適した回避策を確認してから、実際に配備することを推奨いたします。

一般的なワームの軽減

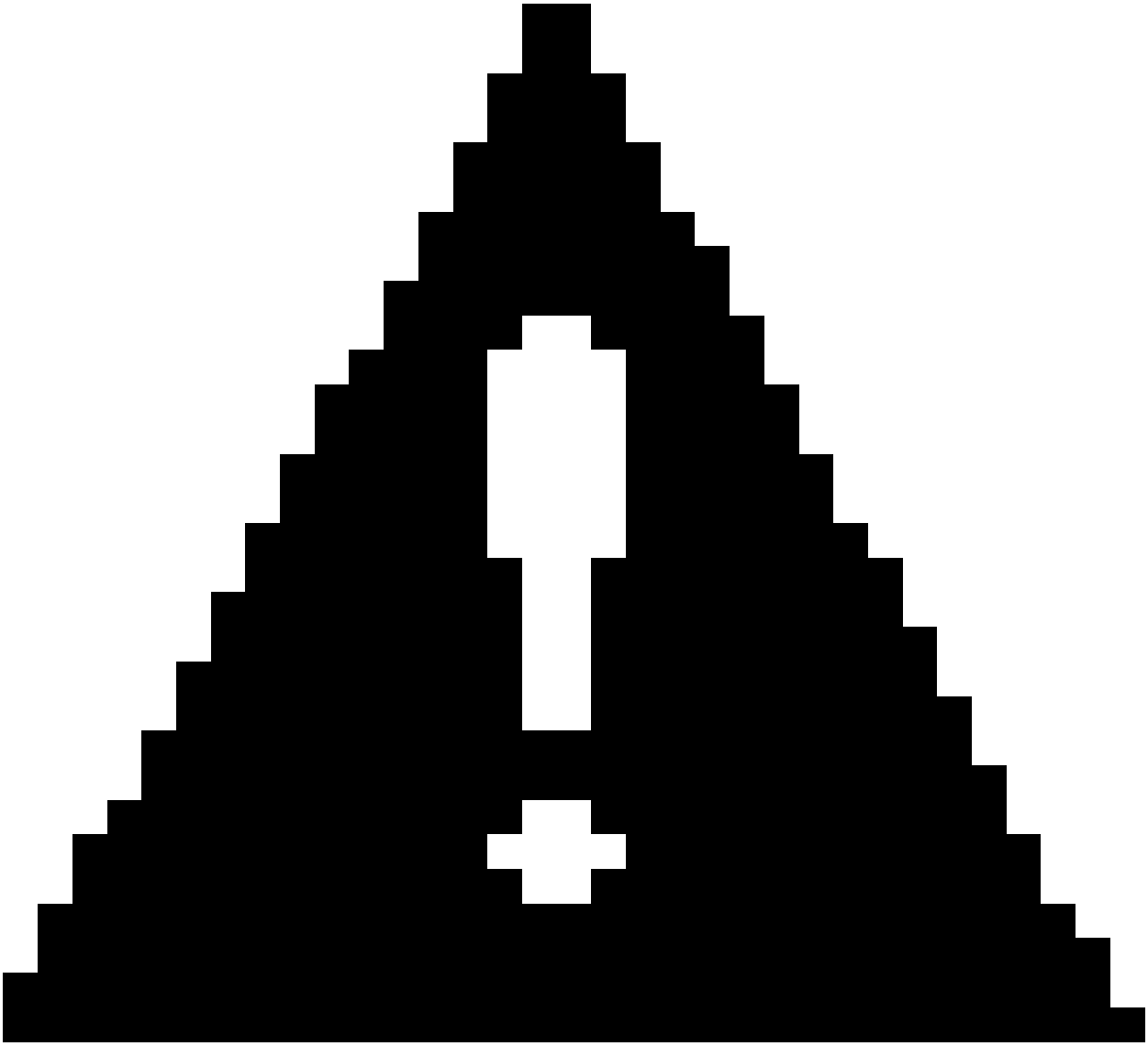
ワームを軽減するための戦略とテクノロジーに関する一般的な情報については、Cisco MySDNサイト(http://www.cisco.com/web/about/security/intelligence/worm-mitigation-whitepaper.html)を参照してください。

Cisco ASAおよびPIXファイアウォール
Cisco侵入防御システム(IPS)
Cisco Security Agent（CSA）
Cisco VPNターミネーションポイント
インターフェイスアクセスリスト
NetFlow

追加情報

Cisco ASAおよびPIXファイアウォール

PIX 6.x



注意：ネットワークの設定変更と同様に、変更を適用する前にこの設定の影響を評価してください。

次に示すアクセスリストエントリには、現在追跡中のワームの亜種の1つの例が含まれています。異なるポートを使用する新しいバリアントも可能であり、例として次の情報を使用してフィルタリングする必要があります。

次のアクセスリストを6.xソフトウェアが稼働するPIX Firewallに適用すると、お客様のネットワークでのMS06-040の悪用の拡散を防止または抑制できます。

PIX 6.x：ネットワーク入力着信フィルタリング

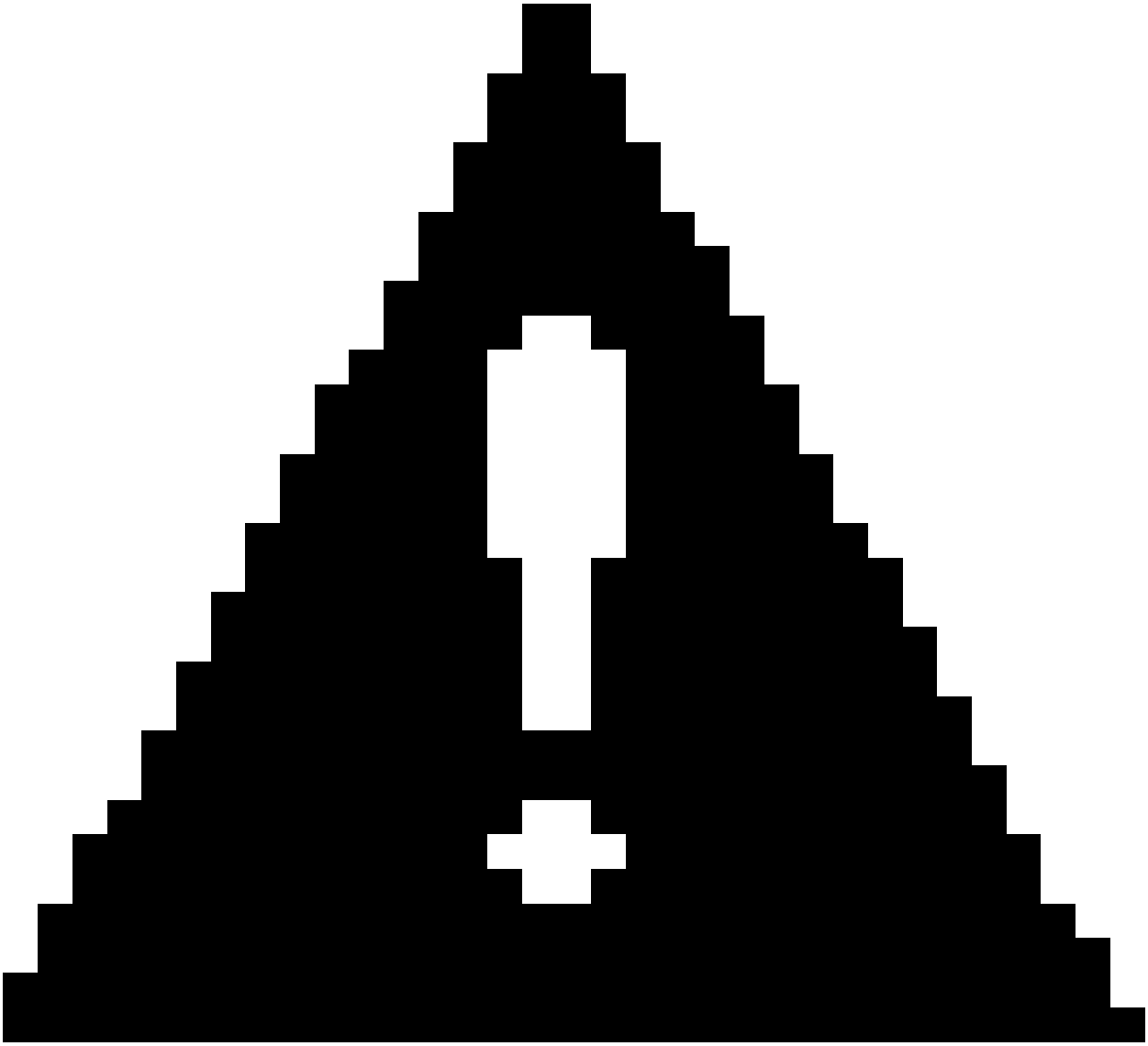
```
!-- MS06-040 - Block Initial Scanning On Internet-facing Interfaces !-- Note: When blocking TCP/139 and
```

```
access-list ms06-040-in deny tcp any any eq netbios-ssn
access-list ms06-040-in deny tcp any any eq 445

!-- Block IRCBot.ST (aka W32.Wargbot, IRC-Mocbot!MS06-040, !-- W32/Cuebot-L, Backdoor.Win32.IRCBot.st,

access-list ms06-040-in deny tcp any any eq 18067

!-- Permit other traffic here.

access-list ms06-040-in permit ip any any


access-group ms06-040-in in interface outside
```

PIX 6.x：ネットワーク入力アウトバウンドフィルタリング

```
!-- MS06-040 - Block Initial Scanning By Infected Hosts

access-list ms06-040-out deny tcp any any eq netbios-ssn
access-list ms06-040-out deny tcp any any eq 445

!-- Block IRCBot.ST (aka W32.Wargbot, IRC-Mocbot!MS06-040, !-- W32/Cuebot-L, Backdoor.Win32.IRCBot.st,

access-list ms06-040-out deny tcp any any eq 18067

!-- Permit other traffic here.

access-list ms06-040-out permit ip any any


access-group ms06-040-out in interface inside
```

PIX/ASA 7.x



注意：ネットワークの設定変更と同様に、変更を適用する前にこの設定の影響を評価してください。

次に示すアクセスリストエントリには、現在追跡中のワームの亜種の1つの例が含まれています。異なるポートを使用する新しいバリアントも可能であり、例として次の情報を使用してフィルタリングする必要があります。

次のアクセスリストを7.xソフトウェアが稼働するPIX/ASAファイアウォールのインバウンドに適用すると、お客様のネットワークでのMS06-040の悪用の拡散を防止または抑制できます。

PIX/ASA 7.x：ネットワーク入力着信フィルタリング

```
!-- MS06-040 - Block Initial Scanning On Internet-facing Interfaces !-- Note: When blocking TCP/139 and
```

```
access-list ms06-040-in extended deny tcp any any eq netbios-ssn
access-list ms06-040-in extended deny tcp any any eq 445

!-- Block IRCBot.ST (aka W32.Wargbot, IRC-Mocbot!MS06-040, !-- W32/Cuebot-L, Backdoor.Win32.IRCBot.st,

access-list ms06-040-in extended deny tcp any any eq 18067

!-- Permit other traffic here.

access-list ms06-040-in extended permit ip any any


access-group ms06-040-in in interface outside
```

PIX/ASA 7.x：ネットワーク入力アウトバウンドフィルタリング

```
!-- MS06-040 - Block Initial Scanning By Infected Hosts

access-list ms06-040-out extended deny tcp any any eq netbios-ssn
access-list ms06-040-out extended deny tcp any any eq 445

!-- Block IRCBot.ST (aka W32.Wargbot, IRC-Mocbot!MS06-040, !-- W32/Cuebot-L, Backdoor.Win32.IRCBot.st,

access-list ms06-040-out extended deny tcp any any eq 18067

!-- Permit other traffic here.

access-list ms06-040-out extended permit ip any any


access-group ms06-040-out in interface inside
```

Cisco侵入防御システム(IPS)

緩和

Cisco Intrusion Prevention System(IPS)は、5.xデバイスのシグニチャパックS243以降でMS06-040の脆弱性を検出できます。

- シグニチャパックS243
  - シグニチャ5799/0 ~ 5799/6を追加
- シグニチャパックS244
  - メタシグニチャ5799/7を追加
  - 変更されたシグニチャ5799/2
  - 廃止されたシグニチャ5799/0および5799/3
- シグニチャパックS245

- WORM_IRCBOT.JKボットネットネットワークのC&Cチャネルに対するDNS要求を検出するためのシグニチャ6013/0を追加
- 変更されたシグニチャ5799/4および5799/7

Cisco Intrusion Detection System(IDS)は、4.xデバイスのシグニチャパックS245以降でMS06-040の脆弱性を検出できます。

- シグニチャパックS245
  - シグニチャ5799/0を追加（デフォルトでは無効）
  - WORM_IRCBOT.JKボットネットネットワークのC&Cチャネルに対するDNS要求を検出するためのシグニチャ6013/0を追加

予防制御をトリガーするには、IPS 5.xシグニチャ5799/4および5799/7またはIDS 4.xシグニチャ5799/0が応答動作を実行するように設定する必要があります。インライン モードで展開されたIPS デバイスを使用している場合、この種の緩和策を提供する処理はさらに効果的になります。この脅威はTCPベースであるため、攻撃がスプーフィングされる可能性はほとんどありません。

識別子

IPSメタシグニチャ5799/4および5799/7は、リモートコード実行攻撃を示す可能性があるWindows Serverサービスの脆弱性の潜在的な不正利用に対して重大度「High」のアラームをトリガーします。サポートするコンポーネントシグニチャは、攻撃の中間ステップを検出するために使用されます。

次のイベントは、IPアドレス192.0.2.157のターゲットの標的に対してWindows Serverサービスの潜在的な不正利用が試みられた後に、シグニチャ5799/7によってトリガーされたものです。

<#root>

```
evIdsAlert: eventId=1154989166673222106 severity=
```

high

```
 vendor=Cisco
    originator:
    hostId: IDSM2
    appName: sensorApp
    appInstanceId: 2972
    time: 2006/08/10 17:41:10 2006/08/10 17:41:10 UTC
    signature: description=Server Service Code Execution id=
```

5799

```
 version=S244
      subsigId:
```

7

```
    sigDetails: Server Service Code Execution
    interfaceGroup:
    vlan: 0
```

```
    participants:
    attacker:
    addr: locality=OUT 192.0.2.157
    <TriggerPacket removed>
    riskRatingValue: 75
    interface: ge0_7
    protocol: IP protocol 0
```

署名の概要

シグニチャパックS243、S244、S245には多数のシグニチャが定義されている。これらのシグニチャのうち、IPS 5.xのお客様はシグニチャ5799/4、5799/7および6013/0を監視する必要があり、IDS 4.xのお客様は5799/0および6013/0を監視する必要があります。残りのIPS 5.x 5799/xシグニチャは、攻撃の個々のステップを特定するコンポーネントです。シグニチャ5799/0および5799/3は、シグニチャパックS244で廃止されます。

さらに、シグニチャ11203/0（重大度：MEDIUM、デフォルトで有効）を変更して、TCPポート18067および22522での潜在的なIRCボットアクティビティを検出できます。シグニチャ11203/0で使用されるサービスポート（TCPポート6666、6667、および6668はデフォルトですでに設定されています）にTCP 18067および22522を追加するには、次の手順を実行します。

IPS 5.xシグニチャ11203/0の変更例

```
<#root>

IPS#

config t

IPS(config)#

service signature-definition sig0


IPS(config-sig)#

signatures 11203 0


IPS(config-sig-sig)#

engine string-tcp

IPS(config-sig-sig-str)#

service-ports 6666-6666,6667-6667,6668-6668,18067-18067,22522-22522

IPS(config-sig-sig-str)#

exit

IPS(config-sig-sig)#

exit
```

```
IPS(config-sig)#
exit
Apply Changes:?[yes]:
yes
IPS(config)#
exit
IPS#
```

IDS 4.xシグニチャ11203/0の変更例

<#root>

```
IPS#
config t
IDS(config)#
service virtual-sensor-configuration virtualSensor

IDS(config-vsc)#
tune-micro-engines

IDS(config-vsc-virtualSensor)#
string.tcp

IDS(config-vsc-virtualSensor-STR)#
signatures SIGID 11203

IDS(config-vsc-virtualSensor-STR-sig)#
servicePorts 6666,6667,6668,18067,22522
IDS(config-vsc-virtualSensor-STR-sig)#
exit

IDS(config-vsc-virtualSensor-STR)#
exit

IDS(config-vsc-virtualSensor)#
exit

Apply Changes:?[yes]:
yes
```

```
IDS(config-vsc)#
exit

IDS(config)#
exit

IDS#
```

注：TCPポート18067と22522はIRC Bot Command & Control channelの新しい/変更されたボットで最も一般的に使用されていますが、異なるポート番号を使用する場合があります。

IDS 4.xシグニチャ

シグニチャパックS245は、Cisco Intrusion Detection(IDS)4.Xデバイス用のシグニチャ5799/0を追加します。ただし、IPS 5.xで使用できる拡張機能により、このシグニチャの検出アルゴリズムはIDS 4.xプラットフォームとIPS 5.xプラットフォームでは異なります。IDS 4.xデバイスでは、5799/0シグニチャは誤検出が発生しやすいため、デフォルトで無効になっています。トラフィックフローによっては、シグニチャ5799/0がローエンドの4.x IDSデバイスのパフォーマンスを低下させる可能性があります。

```
Signature 5799/0 [In IDS 4.x]  Severity: HIGH [Disabled by default]
      engine: STRING.TCP
      ports 139 and 445
```

Cisco Security Agent（CSA）

緩和

Cisco Security Agent(CSA)は、バッファオーバーフロー保護メカニズムを通じて、不正利用による損害を防ぐ緩和策を提供します。これらのメカニズムはデフォルトのルールセットの一部であり、デフォルトで有効になっています。CSAバージョン4.0.3.X以降には、防止機能があります。

CSAエージェントは、この不正利用を正しく防止するために、(「テストモード」ではなく)保護モードに設定する必要があります。更新は不要です。この不正利用を阻止する具体的なルールは次のとおりです。

バッファオーバーフロー保護が見つかりました：

システムAPI制御ルール：ルールモジュール「General Application Permissions - all Security Levels」にあります。このルールの説明は、「ネットワークアプリケーション、アクセスシステ

ム機能はバッファから」です。

ネットワークアクセス制御は次の場所にあります。

ネットワークアクセス制御ルール：ルールモジュール「システム強化モジュール」にあります。このルールの説明：「すべてのアプリケーション、サーバーSMBヌルセッション」

Network access control rule：ルールモジュール「Personal Firewall Module」内にあります。このルールの説明は、「All applications, server for TCP and UDP services」です。

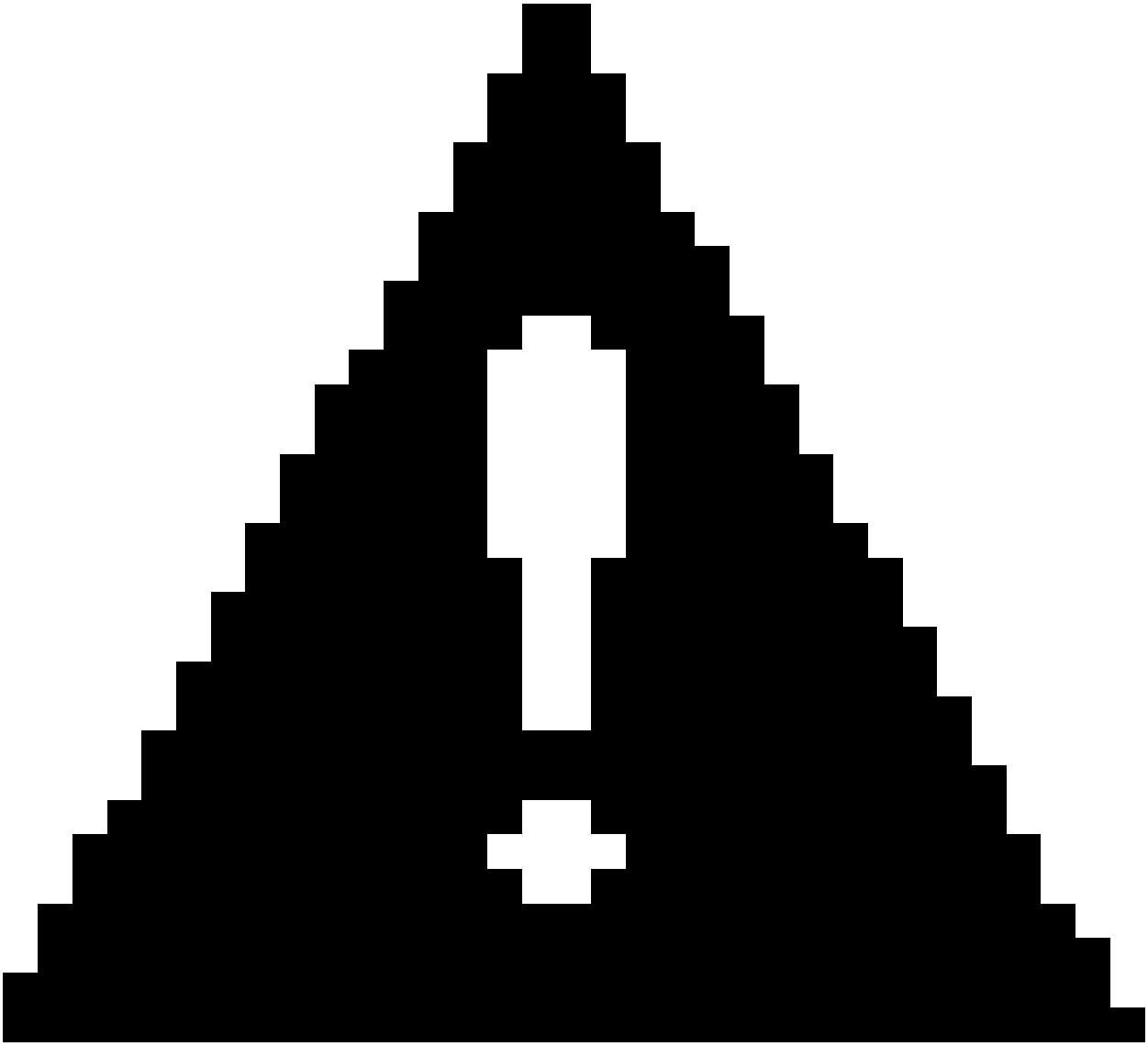
識別子

次のスクリーンショットは、エンドホストでトリガーされたCSAルールを示すCSA Management Center(CSAMC)コンソールを示しています。

Cisco VPNターミネーションポイント

緩和

サイト間VPNでは、暗黙的な信頼モデルではなく、知る必要のあるベースでアクセスコントロールを適用する必要があります。したがって、業務上の使用で特に指示がない限り、標準VPN設定の一部としてTCP/139およびTCP/445をブロックするようにACLを適用することをお勧めします。次に示すIOS ACLの例は、復号化されたVPNトラフィックがVPN終端デバイスを出る際、またはVPN終端デバイスからネクストホップにある別のスクリーニングデバイスを出る際に、このトラフィックに適用される可能性があります。



注意：ネットワークの設定変更と同様に、変更を適用する前にこの設定の影響を評価してください。

次に示すアクセスリストエントリには、現在追跡中のワームの亜種の1つの例が含まれています。異なるポートを使用する新しいバリアントも可能であり、例として次の情報を使用してフィルタリングする必要があります。

追加されたアクセスリストエントリは、ネットワーク入力ポイントでトランジットトラフィックとエッジトラフィックをフィルタリングするトランジットアクセスコントロールリスト(TACL)の一部として実装する必要があります。

tACLについての詳細は、『トランジットアクセスコントロールリスト：エッジでのフィルタリング』を参照してください。

注：送信元アドレスを追跡する場合、アクセスリストの「log」文ではなくSampled NetFlowを使

用してください。log文と高トラフィックが組み合わさってルータに過大な負荷がかかる可能性があります。show access-listコマンドを使用すると、個々のアクセスリストエントリに対するヒットカウントを調べることができます。このデータをSampled NetFlowと組み合わせて使用すると、ネットワークを攻撃している特定のワームの種類を判別できます。

ネットワーク入力着信フィルタリング

```
!-- MS06-040 - Block Initial Scanning On Internet-facing Interfaces !-- Note: When blocking TCP/139 and

access-list 101 deny tcp any any eq 445
access-list 101 deny tcp any any eq 139

!-- Block IRCBot.ST (aka W32.Wargbot, IRC-Mocbot!MS06-040, !-- W32/Cuebot-L, Backdoor.Win32.IRCBot.st,

access-list 101 deny tcp any any eq 18067

!-- Permit other traffic here, !-- or include other Transit ACL entries.

access-list 101 permit ip any any
```

ネットワーク入力アウトバウンドフィルタリング

```
!-- MS06-040 - Block Initial Scanning By Infected Hosts

access-list 110 deny tcp any any eq 139
access-list 110 deny tcp any any eq 445

!-- Block outbound IRC Requests to attacking IRCBot.ST !-- (aka W32.Wargbot, IRC-Mocbot!MS06-040, W32/C

access-list 110 permit tcp <trusted network address block>
      <trusted network block wildcard> any eq 18067 established
access-list 110 deny tcp any any eq 18067

!-- Permit other traffic here,!-- or include other Transit ACL entries.

access-list 110 permit ip any any

!-- Apply the access-lists to the interface.

interface serial 2/0
ip access-group 101 in
ip access-group 110 out
```

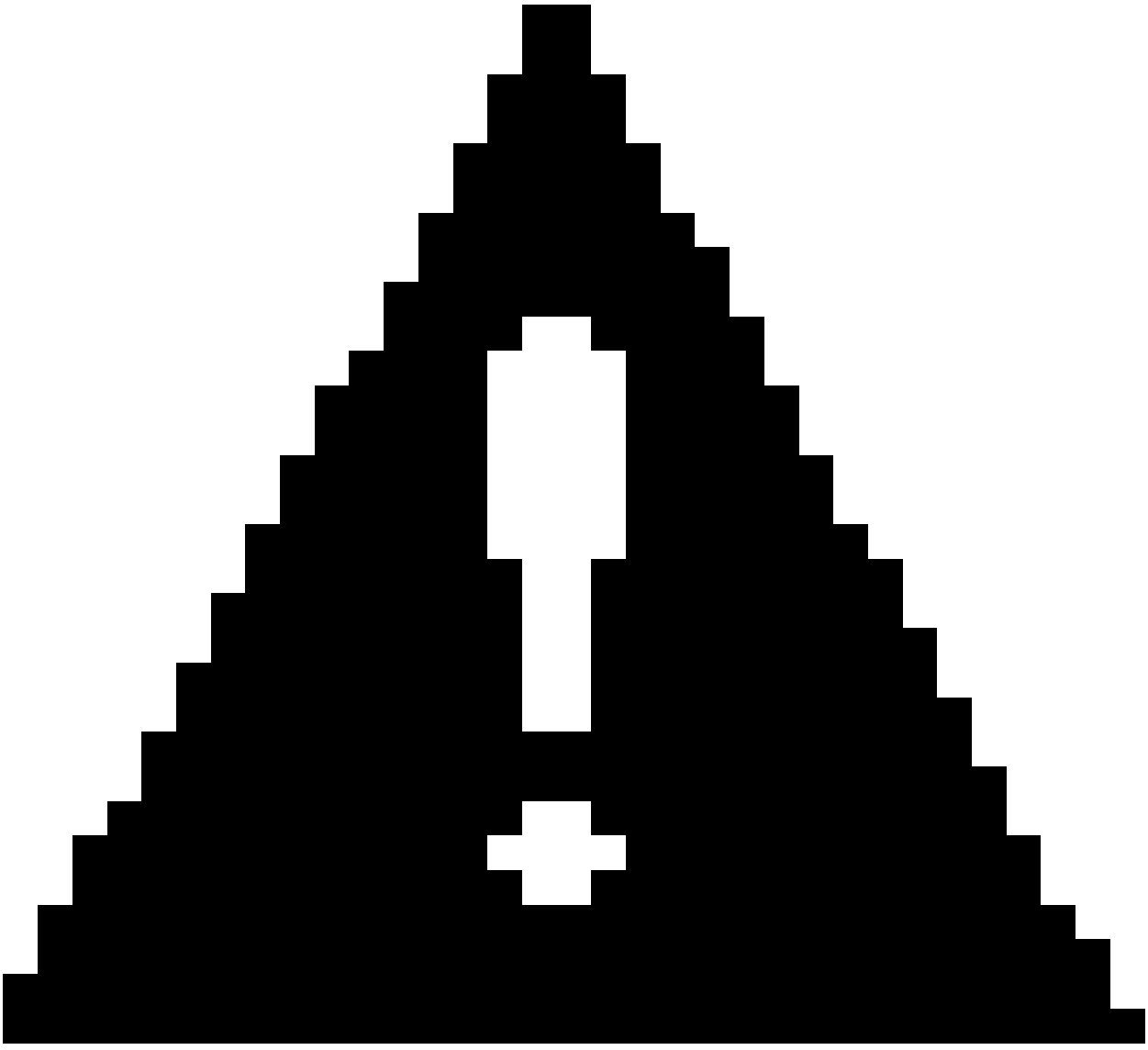
インターフェイスアクセスリスト

アクセスコントロールを提供できるデバイスはすべて、この問題の不正利用の試みを阻止する目

的で配置されます。

緩和

トランジットアクセスリストを使用すると、Cisco IOSルータでインターフェイスアクセスリストを設定して、この問題を悪用（および拡散を阻止）するために使用される可能性のあるパケットを廃棄できます。



注意：ネットワークの設定変更と同様に、変更を適用する前にこの設定の影響を評価してください。

次に示すアクセスリストエントリには、現在追跡中のワームの亜種の1つの例が含まれています。異なるポートを使用する新しいバリアントも可能であり、例として次の情報を使用してフィルタリングする必要があります。

追加されたアクセスリストエントリは、ネットワーク入力ポイントでトランジットトラフィック

とエッジトラフィックをフィルタリングするトランジットアクセスコントロールリスト(TACL)の一部として実装する必要があります。

tACLについての詳細は、『トランジットアクセスコントロールリスト：エッジでのフィルタリング』を参照してください。

注：送信元アドレスを追跡する場合、アクセスリストの「log」文ではなくSampled NetFlowを使用してください。log文と高トラフィックが組み合わさってルータに過大な負荷がかかる可能性があります。show access-listコマンドを使用すると、個々のアクセスリストエントリに対するヒットカウントを調べることができます。このデータをSampled NetFlowと組み合わせて使用すると、ネットワークを攻撃している特定のワームの種類を判別できます。

ネットワーク入力着信フィルタリング

```
!-- MS06-040 - Block Initial Scanning On Internet-facing Interfaces !-- Note: When blocking TCP/139 and

access-list 101 deny tcp any any eq 445
access-list 101 deny tcp any any eq 139

!-- Block IRCBot.ST (aka W32.Wargbot, IRC-Mocbot!MS06-040, !-- W32/Cuebot-L, Backdoor.Win32.IRCBot.st,

access-list 101 deny tcp any any eq 18067

!-- Permit other traffic here,!-- or include other Transit ACL entries.

access-list 101 permit ip any any
```

ネットワーク入力アウトバウンドフィルタリング

```
!-- MS06-040 - Block Initial Scanning By Infected Hosts

access-list 110 deny tcp any any eq 139
access-list 110 deny tcp any any eq 445

!-- Block outbound IRC Requests to attacking IRCBot.ST !-- (aka W32.Wargbot, IRC-Mocbot!MS06-040, W32/C

access-list 110 permit tcp <trusted network address block>
     <trusted network block wildcard> any eq 18067 established
access-list 110 deny tcp any any eq 18067

!-- Permit other traffic here,!-- or include other Transit ACL entries.

access-list 110 permit ip any any

!-- Apply the access-lists to the interface.

interface serial 2/0
```

```
ip access-group 101 in
ip access-group 110 out
```

インターフェイス アクセス リストを使用してトラフィックのフィルタリングを行うと、ICMP 到達不能メッセージが、フィルタリングされたトラフィックの送信元に返されることに注意してください。これは、デバイスがこれらのICMP到達不能メッセージを生成する必要があるため、高いCPU使用率の望ましくない副作用を引き起こす可能性があります。Cisco IOSソフトウェアでは、ICMP到達不能メッセージの生成は500ミリ秒につき1パケットに制限されています。ICMP到達不能メッセージの生成を無効にするには、インターフェイスコンフィギュレーションコマンドno ip unreachablesを使用します。ICMP到達不能レート制限をデフォルトの500ミリ秒あたり1から変更するには、グローバルコンフィギュレーションコマンドip icmp rate-limit unreachable <1-4294967295 millisecond> を使用します。

識別子

トランジットアクセスリストを使用する場合は、インターフェイスアクセスリストを展開した後にshow access-list 101コマンドを使用して、廃棄されているパケットの数を確認できます。ドロップされたパケットを調査して、問題を悪用しようとしていないかどうかを判断する必要があります。

show access-list 101の出力例を次に示します。

<#root>

```
Edge-Router#
```

show access-list 101

```
Extended IP access list 101
10 deny tcp any any eq 445 (141 matches)
20 deny tcp any any eq 139 (100 matches)
30 deny tcp any any eq 18067
40 permit ip any any
```

上記の例では、インターフェイスserial 2/0でインバウンドに設定されたアクセスリストによって、100個のTCP/139パケットと141個のTCP/445パケットが廃棄されています。

NetFlow

インターネットエッジおよびVPN終端ルータでNetFlowを設定して、この脆弱性を不正利用する試みが進行中であるかどうかを確認できます。

<#root>

```
SC1-Cat6506a#
```

show ip cache flow

```
------------------------------------------------------------------------------
MSFC:
IP packet size distribution (2384 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .962 .036 .001 .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
  62 active, 65474 inactive, 2300 added
  42112 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 270664 bytes
  62 active, 16322 inactive, 2300 added, 2300 added to flow
  0 alloc 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  /Pkt     /Sec     /Flow     /Flow
TCP-other         2232      0.0         1    40      0.0       0.0      15.5
ICMP                 6      0.0        15    84      0.0      14.7      15.5
Total:            2238      0.0         1    41      0.0       0.0      15.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Pkts
Vl936         192.0.2.6       Vl600         10.89.236.52    06 1E19 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.78    06 1D07 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.94    06 1C2A 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.102   06 1DD4 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.118   06 1DA0 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.134   06 1D4E 01BD  1
Vl936         192.0.2.6       Vl600         10.89.236.150   06 1C0C 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.174   06 1C04 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.190   06 1D76 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.206   06 1A6A 01BD  1
Vl936         192.0.2.6       Vl600         10.89.236.222   06 1A03 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.230   06 1B84 01BD  1
---------- Output Truncated ----------
```

上記の例では、単一のIPアドレスから複数の宛先IPアドレスへのTCP/139（16進数008B）およびTCP/445（16進数01BD）でのフローの数が非常に多くなっています。インターネットエッジルータ、および場合によってはVPN終端ルータでは、この脆弱性を悪用しようとする試みを示している可能性があり、監視デバイス上のこれらのポートのベースライン使用率と比較する必要があります。

TCP/139（16進数008B）およびTCP/445（16進数01BD）のフローだけを表示するには、show ip cache flowコマンドを使用します。 | inc Srclf|008B|01BDは次のように使用できます。

```
SC1-Cat6506a#

show ip cache flow | inc SrcIf|008B|01BD

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Pkts
Vl936         192.0.2.6       Vl600         10.89.236.52    06 1E19 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.78    06 1D07 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.94    06 1C2A 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.102   06 1DD4 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.118   06 1DA0 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.134   06 1D4E 01BD  1
Vl936         192.0.2.6       Vl600         10.89.236.150   06 1C0C 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.174   06 1C04 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.190   06 1D76 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.206   06 1A6A 01BD  1
Vl936         192.0.2.6       Vl600         10.89.236.222   06 1A03 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.230   06 1B84 01BD  1
Vl936         192.0.2.6       Vl600         10.89.236.246   06 1928 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.6     06 19AB 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.22    06 18ED 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.46    06 1997 01BD  1
Vl936         192.0.2.6       Vl600         10.89.236.161   06 1757 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.221   06 17E3 008B  1
Vl936         192.0.2.6       Vl600         10.89.236.77    06 17D6 008B  1
---------- Output Truncated ----------
```

シスコのセキュリティ手順

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 https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.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。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060814-ms06-040-vulnerability

改訂履歴

バージョン	説明	セクション	日付
リビジョン 1.1	Cisco ASAおよびPIXファイアウォール、Cisco Intrusion Prevention System、Cisco Security Agent、Cisco VPNターミネーションポイント、インターフェイスアクセスリストの緩和策に関する情報を更新。NetFlowのセクションを追加。		2006年8月21日
リビジョン 1.0	初回公開リリース		2006年8月14日

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。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。