Cisco Network Admission Control Managerのディレクトリトラバーサルの脆弱性が悪用される問題の識別と影響の緩和

Cisco Network Admission Control Managerのディレクトリトラバーサルの脆弱性が悪用される問題の識別と影響の緩和

Advisory ID:cisco-amb-20111005-nac

http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20111005-nac

リビジョン 1.1

最終更新日：2011年10月18日17:06 UTC(GMT)

一般公開2011年10月5日16:00 UTC(GMT)

目次

Cisco の対応

この適用対応策速報は、*Cisco Network Admission Control Manager*のPSIRTセキュリティアドバイザリ*ディレクトリトラバーサルの脆弱性*の関連ドキュメントで、管理者がCiscoネットワークデバイスに導入できる識別および緩和策を提供します。

脆弱性の特性

Cisco Network Admission Control Manager(Cisco NAC Manager)には、ディレクトリトラバーサルの脆弱性があります。この脆弱性は、認証なしでリモートから悪用される可能性があり、エンドユーザの操作が必要です。この脆弱性の不正利用に成功すると、情報の開示が可能になり、攻撃者は該当デバイスやネットワークに関する情報を学習できるようになります。この脆弱性を悪用するための攻撃方法は、TCPポート443を使用するHTTPSパケットを使用することです。

この脆弱性には、CVE 識別子 CVE-2011-3305 が割り当てられています。

脆弱性の概要

脆弱性のあるソフトウェア、該当しないソフトウェア、修正済みソフトウェアについては、次の PSIRT セキュリティ アドバイザリを参照してください。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111005-nac にアクセスしてください。

緩和テクニックの概要

シスコデバイスには、この脆弱性に対する複数の対応策があります。これらの保護方法は、インフラストラクチャ デバイスとネットワークを通過するトラフィックのセキュリティを保護する一般的なベスト プラクティスであると考えられます。このセクションでは、これらのテクニックの概要について説明します。

Cisco IOSソフトウェアは、インフラストラクチャアクセスコントロールリスト(iACL)を使用して、悪用を効果的に防止できます。 この保護メカニズムは、この脆弱性を悪用しようとしているパケットをフィルタリングして廃棄します。

Cisco ASA 5500シリーズ適応型セキュリティアプライアンス、適応型セキュリティアプライアンスサービスモジュール(ASASM)、およびCisco Catalyst 6500シリーズスイッチおよびCisco 7600シリーズルータでは、トランジットアクセスコントロールリスト(tACL)を使用してFirewall Services Module(FWSM)を使用することもできます。を参照)。 この保護メカニズムは、この脆弱性を悪用しようとしているパケットをフィルタリングして廃棄します。

Cisco IOS NetFlowレコードは、ネットワークベースの不正利用の試みを可視化できます。

Cisco IOSソフトウェア、Cisco ASAアプライアンス、ASASM、およびFWSMファイアウォールは、syslogメッセージと**show**コマンドの出力に表示されるカウンタ値を通じて可視性を提供できます。

リスク管理

組織は、リスク評価および軽減の標準プロセスに従って、[この脆弱性|これらの脆弱性]の潜在的な影響を判断することを推奨します。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。 セキュリティ脆弱性に関するリスクトリアージの発表と リスクトリアージおよびプロトタイピングは、繰り返し可能なセキュリティ評価および対応プロセスの開発に役立ちます。

デバイス別の緩和策と識別策

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。

ここでは緩和策と識別策に関する情報が次のデバイス別に提供されています。

- Cisco IOSルータおよびスイッチ
- Cisco IOS NetFlow
- Cisco ASA、ASASM、およびFWSMファイアウォール

Cisco IOS ルータおよびスイッチ

緩和策：インフラストラクチャ アクセス コントロール リスト

インフラストラクチャデバイスを保護し、直接インフラストラクチャ攻撃のリスク、影響、および効果を最小限に抑えるために、インフラストラクチャ機器に送信されるトラフィックのポリシー適用を実行するiACLを導入することを推奨します。iACL は、既存のセキュリティ ポリシーと設定に基づいて、インフラストラクチャ デバイス宛ての正当なトラフィックのみを明示的に許可することによって構築されます。インフラストラクチャ デバイスの保護を最大にするには、IP アドレスが設定されているすべてのインターフェイスの入力方向で配備済みの iACL を適用する必要があります。iACLの回避策では、信頼できる送信元アドレスから攻撃が発生した場合に、この脆弱性に対する完全な保護を提供できません。

iACLポリシーは、影響を受けるデバイスに送信されるTCPポート443の不正なHTTPSパケットを拒否します。次の例では、192.168.60.0/24が影響を受けるデバイスによって使用されるIPアドレス空間であり、192.168.100.1のホストは影響を受けるデバイスへのアクセスを必要とする信頼できる送信元と見なされます。許可されないすべてのトラフィックを拒否する前に、ルーティングおよび管理アクセスに必要なトラフィックを許可するように注意する必要があります。インフラストラクチャのアドレス レンジは、できるだけユーザおよびサービス セグメントに使用されるアドレス レンジとは別個にする必要があります。このようにアドレスを設定することで、iACL の構築と配備が容易になります。

iACLについての詳細は、『コアの保護：インフラストラクチャ保護 ACL』を参照してください。

```
 ip access-list extended Infrastructure-ACL-Policy
 !
!-- Include explicit permit statements for trusted sources
!-- that require access on the vulnerable port
!
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
 !
!-- The following vulnerability-specific access control entry
!-- (ACE) can aid in identification of attacks
!
deny tcp any 192.168.60.0 0.0.0.255 eq 443
 !
!-- Explicit deny ACE for traffic sent to addresses configured within
!-- the infrastructure address space
!
deny ip any 192.168.60.0 0.0.0.255
!
!-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations
!
!-- Apply iACL to interfaces in the ingress direction
!
interface GigabitEthernet0/0
ip access-group Infrastructure-ACL-Policy in
```

インターフェイス アクセス リストを使用して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ようになります。これらのメッセ

ージを生成すると、デバイスの CPU 使用率が上昇する可能性があります。Cisco IOS ソフトウェアでの ICMP 到達不能メッセージの生成は、デフォルトで 500 ミリ秒につき 1 パケットまで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設定から変更するには、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** *interval-in-ms* を使用します。

識別策：インフラストラクチャ アクセス コントロール リスト

管理者がiACLをインターフェイスに適用すると、**show ip access-lists**コマンドによって、iACLが適用されているインターフェイスでフィルタリングされたTCPポート443のHTTPSパケットの数が識別されます。フィルタリングされたパケットに対しては、この脆弱性を悪用しようとしていないかどうかを調査する必要があります。次に **show ip access-lists Infrastructure-ACL-Policy** の出力例を示します。

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
20 deny tcp any 192.168.60.0 0.0.0.255 eq 443 (17 matches)
30 deny ip any 192.168.60.0 0.0.0.255
router#
```

前記の例では、アクセスリスト*Infrastructure-ACL-Policy*により、**TCP**ポート**443**で**17**個のHTTPSパケットが**ACE**の**アクセスコントロールリストエントリ**(ACE)行2で廃棄されました。

ACEカウンタとsyslogイベントを使用してインシデントを調査する詳細については、『ファイアウォールとIOSルータsyslogイベントを使用したインシデントの特定Applied Intelligence white paper』を参照してください。

管理者は、Embedded Event Manager(EEM)を使用して、ACEカウンタのヒットなどの特定の条件が満たされた場合に計測機能を提供できます。Applied Intelligence white paper Embedded Event Manager in a Security Contextでは、この機能の使用方法に関する詳細を説明しています。

識別策：アクセス リスト ロギング

log および **log-input** アクセス コントロール リスト（ACL）オプションを使用すると、特定の ACE に一致するパケットがログに記録されます。**log-input** オプションを使用すると、パケットの送信元および宛先の IP アドレスとポートに加え、入力インターフェイスのロギングが有効になります。

注意：アクセス コントロール リストのロギングは CPU に多大な負荷を与えることがあるので、使用する場合は細心の注意を払う必要があります。ACL ロギングによる CPU への影響を左右する要素は、ログの生成、ログの送信、およびログが有効な ACE に一致するパケットを転送するプロセス交換です。

Cisco IOS ソフトウェアでは、**ip access-list logging interval** *interval-in-ms* コマンドを使用すると、ACL ロギングによって引き起こされるプロセス交換の影響を制限できます。**logging rate-limit** *rate-per-second* [**except** *loglevel*] コマンドを使用すると、ログの生成と送信の影響を制限できます。

Supervisor Engine 6500 または Supervisor Engine 7600 を搭載した Cisco Catalyst 720 シリーズ スイッチおよび Cisco 32 シリーズ ルータでは、ACL ロギングによる CPU への影響をハードウェアで最適化することができます。

ACL ロギングの設定と使用についての詳細は、Applied Intelligence white paper『アクセス コントロール リストのログについて』を参照してください。

Cisco IOS NetFlow

識別策：NetFlow レコードを使用したトラフィック フローの識別

管理者は、Cisco IOSルータおよびスイッチでCisco IOS NetFlowを設定して、この脆弱性を悪用しようとしている可能性があるトラフィックフローを特定できます。フローを調査して、脆弱性を不正利用しようとする試みなのか、正当なトラフィックフローなのかを判断することを推奨します。

```
router#show ip cache flow
IP packet size distribution (90784136 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .001 .256 .000 .010 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  1885 active, 63651 inactive, 59960004 added
  129803821 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
  0 active, 16384 inactive, 0 added, 0 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-Telnet    11393421      2.8         1    48      3.1       0.0       1.4
TCP-FTP            236      0.0        12    66      0.0       1.8       4.8
TCP-FTPD            21      0.0     13726  1294      0.0      18.4       4.1
TCP-WWW          22282      0.0        21  1020      0.1       4.1       7.3
TCP-X              719      0.0         1    40      0.0       0.0       1.3
TCP-BGP              1      0.0         1    40      0.0       0.0      15.0
TCP-Frag         70399      0.0         1   688      0.0       0.0      22.7
TCP-other     47861004     11.8         1   211     18.9       0.0       1.3
UDP-DNS            582      0.0         4    73      0.0       3.4      15.4
UDP-NTP         287252      0.0         1    76      0.0       0.0      15.5
UDP-other       310347      0.0         2   230      0.1       0.6      15.9
ICMP             11674      0.0         3    61      0.0      19.8      15.5
IPv6INIP            15      0.0         1  1132      0.0       0.0      15.4
GRE                  4      0.0         1    48      0.0       0.0      15.3
Total:        59957957     14.8         1   196     22.5       0.0       1.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.201  Gi0/1         192.168.60.122  06 0984 01BB     9
Gi0/1         192.168.150.60  Gi0/0         10.89.16.226    11 0016 12CA     1
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3E 01BB     5
Gi0/0         192.168.10.17   Gi0/1         192.168.60.77   06 0B89 01BB     4
Gi0/0         10.88.226.1     Gi0/1         192.168.202.22  11 007B 007B     1
```

```
Gi0/0          10.89.16.226    Gi0/1          192.168.150.60  06 12CA 0016     1
router#
```

上の例では、**TCP**ポート443（**16進値01BB**）に**HTTPS**の複数のフロー**があり**ます。

TCPポート443（16進値01BB）でHTTPSパケットのトラフィックフローのみを表示するには、**show ip cache flow**コマンドを使用します。 **| include SrcIf|_06_.*01BB_**は、関連するTCP NetFlowレコードを次のように表示します。

```
router#show ip cache flow | include SrcIf|_06_.*01BB_
SrcIf         SrcIPaddress     DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.201   Gi0/1         192.168.60.122  06 0984 01BB     9
Gi0/0         192.168.13.97    Gi0/1         192.168.60.28   06 0B3E 01BB     5
Gi0/0         192.168.10.17    Gi0/1         192.168.60.77   06 0B89 01BB     4
router#
```

Cisco ASA、ASASM、およびFWSMファイアウォール

緩和策：トランジットアクセスコントロールリスト

インターネット接続ポイント、パートナーとサプライヤの接続ポイント、またはVPN接続ポイントなど、入力アクセスポイントでネットワークに入るトラフィックからネットワークを保護するために、tACLを導入してポリシーを適用することを推奨します。tACL の構築は、既存のセキュリティ ポリシーと設定に基づいて、入力アクセス ポイントからネットワーク内に入ることを許可されたトラフィックのみを明示的に許可するか、ネットワークを通過することを許可されたトラフィックを許可することによって達成されます。tACLの回避策は、信頼できる送信元アドレスから攻撃が発生した場合に、この脆弱性に対する完全な保護を提供できません。

tACLポリシーは、該当デバイスに送信されるTCPポート443の不正なHTTPSパケットを拒否します。次の例では、192.168.60.0/24が影響を受けるデバイスによって使用されるIPアドレス空間であり、192.168.100.1のホストは影響を受けるデバイスへのアクセスを必要とする信頼できる送信元と見なされます。許可されないすべてのトラフィックを拒否する前に、ルーティングおよび管理アクセスに必要なトラフィックを許可するように注意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。

```
!
!-- Include explicit permit statements for trusted sources
!-- that require access on the vulnerable port
! access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 443 !
!-- The following vulnerability-specific access control entries
!-- (ACEs) can aid in identification of attacks
! access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 443 !
!-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations
!
!-- Explicit deny for all other IP traffic
! access-list tACL-Policy extended deny ip any any !
!-- Apply tACL to interface(s) in the ingress direction
! access-group tACL-Policy in interface outside
```

識別策：トランジットアクセスコントロールリスト

tACLをインターフェイスに適用した後、管理者は**show access-list**コマンドを使用して、TCPポート443でフィルタリングされたHTTPSパケットの数を識別できます。フィルタリングされたパケットを調査して、この脆弱性を悪用しようとしていないかどうかを判断することを推奨します。**show access-list tACL-Policy**の出力例を次に示します。

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 3 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq https (hitcnt=34)
access-list tACL-Policy line 2 extended deny tcp any 192.168.60.0 255.255.255.0 eq
https (hitcnt=139)
access-list tACL-Policy line 3 extended deny ip any any (hitcnt=8)
firewall#
```

前記の例では、アクセスリスト*tACL-Policy*によって、信頼できないホストまたはネットワークから受信した**TCPポート443**上の139個のHTTPSパケットが廃棄されています。また、syslog メッセージ 106023 には、送信元と宛先の IP アドレス、送信元と宛先のポート番号、拒否されたパケットの IP プロトコルなど、有益な情報が含まれている場合があります。

識別策：ファイアウォール アクセス リスト syslog メッセージ

log キーワードを含まないアクセス コントロール エントリ（ACE）によって拒否されたパケットに対しては、ファイアウォール syslog メッセージ **106023 が生成されます。**このsyslogメッセージの詳細については、『Ciscoセキュリティアプライアンスシステムログメッセージ：106023』を参照してください。

Cisco ASA 5500シリーズ適応型セキュリティアプライアンスまたはCisco PIX 500シリーズセキュリティアプライアンスのsyslog設定の詳細は、『セキュリティアプライアンスの監視：ログの設定と管理』を参照してください。Cisco Catalyst 6500シリーズスイッチおよびCisco 7600シリーズルータ用FWSMでのsyslogの設定については、『ファイアウォールサービスモジュールのモニタリング』を参照してください。

次の例では、**show logging | grep** regexコマンドは、ファイアウォールのロギングバッファからsyslogメッセージを抽出します。これらのメッセージは、このドキュメントで説明されている脆弱性を悪用しようとする試みの可能性を示す、拒否されたパケットに関する追加情報を提供します。**grep** キーワードを付けて別の正規表現を使用すると、ログ メッセージに含まれる特定のデータを検索できます。

正規表現の構文の詳細は、「正規表現の作成」を参照してください。

```
firewall#show logging | grep 106023
  Oct 05 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.18/2944
         dst inside:192.168.60.191/443 by access-group "tACL-Policy"
  Oct 05 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.205/2945
         dst inside:192.168.60.33/443 by access-group "tACL-Policy"
  Oct 05 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.49/2946
         dst inside:192.168.60.240/443 by access-group "tACL-Policy"
  Oct 05 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.100/2947
         dst inside:192.168.60.115/443 by access-group "tACL-Policy"
  Oct 05 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.88/2949
         dst inside:192.168.60.38/443 by access-group "tACL-Policy"
  Oct 05 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.155/2950
         dst inside:192.168.60.250/443 by access-group "tACL-Policy"
```

```
firewall#
```
前記の例では、tACL *tACL-Policy*に関して口ギングされたメッセージには、**TCPポート443の HTTPS**パケットが、該当デバイスに割り当てられたアドレスブロックに送信されます。

ASAおよびPIXセキュリティアプライアンスのsyslogメッセージの詳細については、『Ciscoセキュリティアプライアンスシステムログメッセージ』を参照してください。FWSMのsyslogメッセージの詳細については、『Catalyst 6500シリーズスイッチとCisco 7600シリーズルータのファイアウォールサービスモジュールロギングシステムログメッセージ』を参照してください。

syslogイベントを使用してインシデントを調査する方法の詳細については、『ファイアウォールとIOSルータsyslogイベントを使用したインシデントの特定Applied Intelligence white paper』を参照してください。

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	2011年10月5日	最初のパブリックリリース

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 http://www.cisco.com/web/about/security/psirt/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。

関連情報

- Cisco 適用対応策速報（英語）
- Cisco IOS デバイスの強化ガイド
- Cisco Security Center
- Cisco IOS NetFlow：Cisco.com のホーム ページ（英語）
- Cisco IOS NetFlow White Paper（英語）
- NetFlowパフォーマンス分析
- Cisco Network Foundation Protection White Paper（英語）
- Cisco Network Foundation Protection プレゼンテーション資料（英語）
- Cisco ファイアウォール製品：Cisco.com のホーム ページ（英語）
- Cisco Security Monitoring, Analysis, and Response System
- Common Vulnerabilities and Exposures（CVE）