Cisco ASA適応型セキュリティアプライアンスおよびCisco PIXセキュリティアプライアンスの複数の脆弱性

アドバイザリーID : cisco-sa-20090408-asa
初公開日 : 2009-04-08 16:00
バージョン 1.2 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID :

CVE-2009-1155
CVE-2009-1159
CVE-2009-1158
CVE-2009-1157
CVE-2009-1156
CVE-2009-1160

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

Cisco ASA 5500 シリーズ 適応型セキュリティアプライアンスおよび Cisco PIX セキュリティアプライアンスに複数の脆弱性が存在しています。このセキュリティアドバイザリでは、これらの脆弱性の詳細について説明します。

- アカウント上書き機能を使用した場合のVPN認証バイパスの脆弱性
- 巧妙に細工されたHTTPパケットによるサービス拒否(DoS)の脆弱性
- 巧妙に細工されたTCPパケットによるDoS脆弱性
- 巧妙に細工されたH.323パケットによるDoSの脆弱性
- SQL*NetパケットのDoS脆弱性
- アクセスコントロールリスト(ACL)バイパスの脆弱性

一部の脆弱性には回避策があります。

このアドバイザリは、
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090408-asa で公開されています。

該当製品

脆弱性のある製品

以下に、本アドバイザリに記載された各脆弱性の影響を受ける製品のリストを示します。

VPN認証バイパスの脆弱性

IPsecまたはSSLベースのリモートアクセスVPN用に設定され、Override Account Disabled機能が有効になっているCisco ASAまたはCisco PIXセキュリティアプライアンスは、この脆弱性の影響を受けます。

注：Override Account Disabled機能は、Cisco ASAソフトウェアバージョン7.1(1)で導入されました。Cisco ASAおよびPIXソフトウェアバージョン7.1、7.2、8.0、および8.1は、この脆弱性の影響を受けます。この機能はデフォルトで無効になっています。

巧妙に細工されたHTTPパケットによるDoS脆弱性

Cisco ASAセキュリティアプライアンスで、SSL VPN用に設定されているか、Cisco Adaptive Security Device Manager(ASDM)接続を受け入れるように設定されている場合、一連の巧妙に細工されたHTTPパケットによってトリガーされるデバイスのリロードが発生する場合があります。この脆弱性の影響を受けるのは、Cisco ASAソフトウェアバージョン8.0および8.1のみです。

巧妙に細工されたTCPパケットによるDoS脆弱性

Cisco ASAおよびCisco PIXセキュリティアプライアンスで、巧妙に細工された一連のTCPパケットによって引き起こされる可能性のあるメモリリークが発生する場合があります。バージョン7.0、7.1、7.2、8.0、および8.1を実行しているCisco ASAおよびCisco PIXセキュリティアプライアンスは、次のいずれかの機能が設定されている場合に影響を受けます。

- SSL VPN
- ASDM管理アクセス
- Telnet 経由のアクセス
- SSHアクセス
- リモートアクセスVPN用のCisco Tunneling Control Protocol(cTCP)
- 仮想 Telnet
- 仮想 HTTP

- 暗号化音声インスペクション用のTransport Layer Security(TLS)プロキシ
- ネットワーク アクセスのカットスルー プロキシ
- TCP 代行受信

巧妙に細工されたH.323パケットによるDoS脆弱性

Cisco ASAおよびCisco PIXセキュリティアプライアンスで、H.323インスペクションが有効になっている場合、一連の巧妙に細工されたH.323パケットによってトリガーされる可能性があるデバイスのリロードが発生する場合があります。H.323インスペクションはデフォルトで有効になっています。Cisco ASAおよびCisco PIXソフトウェアバージョン7.0、7.1、7.2、8.0、および8.1は、この脆弱性の影響を受けます。

SQL*NetパケットのDoS脆弱性

Cisco ASAおよびCisco PIXセキュリティアプライアンスで、SQL*Netインスペクションが有効になっている場合、一連のSQL*Netパケットによってトリガーされる可能性のあるデバイスのリロードが発生する場合があります。SQL*Netインスペクションはデフォルトで有効になっています。Cisco ASAおよびCisco PIXソフトウェアバージョン7.2、8.0、8.1は、この脆弱性の影響を受けます。

アクセスコントロールリストバイパスの脆弱性

Cisco ASAおよびCisco PIXセキュリティアプライアンスには脆弱性があり、デバイス内で設定されたACLの最後でトラフィックが暗黙の拒否をバイパスできる可能性があります。Cisco ASAおよびCisco PIXソフトウェアバージョン7.0、7.1、7.2、および8.0は、この脆弱性の影響を受けます。

ソフトウェアバージョンの確認

show versionコマンドラインインターフェイス(CLI)コマンドを使用すると、脆弱性のあるバージョンのCisco PIXまたはCisco ASAソフトウェアが実行されているかどうかを確認できます。次の例は、ソフトウェアバージョン8.0(4)が稼働するCisco ASA適応型セキュリティアプライアンスを示しています。

```
<#root>

ASA#

show version


    Cisco Adaptive Security Appliance Software Version 8.0(4)
    Device Manager Version 6.0(1)

<output truncated>
```

次の例は、ソフトウェアバージョン8.0(4)が稼働するCisco PIXセキュリティアプライアンスを示しています。

```
<#root>

PIX#

show version


Cisco PIX Security Appliance Software Version 8.0(4)
Device Manager Version 5.2(3)

<output truncated>
```

Cisco ASDMを使用してデバイスを管理している場合は、ログインウィンドウの表またはASDMウィンドウの左上隅に表示されるソフトウェアバージョンを確認できます。

脆弱性を含んでいないことが確認された製品

Cisco Catalyst 6500シリーズスイッチ、Cisco 7600シリーズルータ、Cisco VPN 3000シリーズコンセントレータ用のCisco Firewall Services Module(FWSM)は、これらの脆弱性の影響を受けません。Cisco PIXセキュリティアプライアンスソフトウェアバージョン6.xは、これらの脆弱性の影響を受けません。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。

詳細

このセキュリティ アドバイザリでは、相互に独立した複数の脆弱性が説明されています。これらの脆弱性は相互に関連していません。

VPN認証バイパスの脆弱性

Cisco ASAまたはCisco PIXセキュリティアプライアンスは、AAAサーバからのアカウント無効表示を上書きし、ユーザがログインできるように設定できます。ただし、ユーザがVPNにログインするには、正しいクレデンシャルを入力する必要があります。Cisco ASAおよびCisco PIXセキュリティアプライアンスには、オーバーライドアカウント機能が有効な場合にVPNユーザが認証をバイパスできる脆弱性が存在します。

注：アカウントの上書き機能は、Cisco ASAソフトウェアバージョン7.1(1)で導入されました。

次の例に示すように、アカウントの上書き機能は、tunnel-group general-attributesコンフィギュレーションモードでoverride-account-disableコマンドを使用して有効にします。次の例では、WebVPNトンネルグループ「testgroup」のAAAサーバからの「account-disabled」インジケータの上書きを許可しています。

<#root>

```
hostname(config)#
tunnel-group testgroup type webvpn
hostname(config)#
tunnel-group testgroup general-attributes
hostname(config-tunnel-general)#
override-account-disable
```

注：アカウントの上書き機能はデフォルトで無効になっています。

この脆弱性は、Cisco Bug ID CSCsx47543 (登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2009-1155が割り当てられています。

巧妙に細工されたHTTPパケットによるDoS脆弱性

巧妙に細工されたSSLまたはHTTPパケットにより、SSL VPN接続を終了するように設定されたCisco ASAデバイスでDoS状態が発生する可能性があります。この脆弱性は、ASDMアクセスが有効になっているインターフェイスに対してトリガーされる可能性もあります。攻撃に成功すると、デバイスのリロードが発生する可能性があります。この脆弱性を不正利用するには、TCP 3ウェイハンドシェイクが必要です。

この脆弱性は、Cisco Bug ID CSCsv52239(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2009-1156が割り当てられています。

巧妙に細工されたTCPパケットによるDoS脆弱性

巧妙に細工されたTCPパケットにより、Cisco ASAまたはCisco PIXデバイスでメモリリークが発生する可能性があります。攻撃に成功すると、DoS状態が続く可能性があります。次のいずれかの機能が設定されているCisco ASAデバイスが影響を受けます。

- SSL VPN
- ASDM管理アクセス
- Telnet 経由のアクセス
- SSHアクセス
- リモートアクセスVPN用のcTCP
- 仮想 Telnet
- 仮想 HTTP
- 暗号化された音声検査の TLS プロキシ
- ネットワーク アクセスのカットスルー プロキシ
- TCP 代行受信

注：この脆弱性は、該当デバイスで終端する任意のTCPベースのサービスに巧妙に細工されたパケットが送信されたときにトリガーされる可能性があります。この脆弱性は、TCPインターセプト機能が有効になっている場合にのみ、一時的なトラフィックによって引き起こされる可能性があります。この脆弱性を不正利用するためにTCP 3ウェイハンドシェイクは必要ありません。

この脆弱性は、Cisco Bug ID CSCsy22484 (登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2009-1157が割り当てられています。

巧妙に細工されたH.323パケットによるDoS脆弱性

巧妙に細工されたH.323パケットにより、H.323インスペクションが設定されたCisco ASAデバイスでDoS状態が発生する可能性があります。H.323インスペクションはデフォルトで有効になっています。攻撃に成功すると、デバイスのリロードが発生する可能性があります。この脆弱性を不正利用するためにTCP 3ウェイハンドシェイクは必要ありません。

この脆弱性は、Cisco Bug ID CSCsx32675(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2009-1158が割り当てられています。

SQL*NetパケットのDoS脆弱性

SQL*Netプロトコルは、セキュリティアプライアンスによって処理されるさまざまなパケットタイプで構成されます。これにより、Cisco ASAおよびCisco PIXセキュリティアプライアンスのどちらの側でも、Oracleバージョン7.x以前の実装とデータストリームの一貫性が保たれます。一連のSQL*Netパケットにより、SQL*Netインスペクションが設定されたCisco ASAおよびCisco PIXデバイスでサービス拒否状態が発生する可能性があります。SQL*Netインスペクションはデフォルトで有効になっています。攻撃に成功すると、デバイスのリロードが発生する可能性があります。

SQL*Netのデフォルトのポート割り当てはTCPポート1521です。これは、OracleがSQL*Net用に使用する値です。class-mapコマンドは、Cisco ASAまたはCisco PIXでSQL*Netインスペクションをさまざまなポート番号に適用するために使用できることに注意してください。この脆弱性を不正利用するには、TCP 3ウェイハンドシェイクが必要です。TCP 3ウェイハンドシェイクの要件により、スプーフィングされた送信元アドレスを持つパケットを使用した不正利用の可能性が大幅に低減されます。

この脆弱性は、Cisco Bug ID CSCsw51809(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2009-1159が割り当てられています。

アクセスコントロールリストバイパスの脆弱性

アクセスリストには、ACL内の許可ACEまたは拒否ACEのいずれとも一致せず、ACLの最後に到達するパケットに適用される、暗黙的な拒否動作があります。この暗黙のdenyは意図的に存在しており、設定を必要とせず、ACLの最後に到達するすべてのトラフィックを拒否する暗黙のACEと理解できます。Cisco ASAおよびCisco PIXには、トラフィックが暗黙のdeny ACEをバイ

パスする可能性のある脆弱性が存在します。

注：この動作は、デバイスに適用されるすべてのACLの暗黙のdenyステートメントにのみ影響します。明示的なdenyステートメントを含むアクセスコントロールリスト(ACL)は、この脆弱性の影響を受けません。この脆弱性は非常にまれな状況で発生し、再現が非常に困難です。

セキュリティアプライアンスでパケットの寿命を追跡し、パケットトレーサツールでパケットが正常に動作しているかどうかを確認できます。packet-tracerコマンドは、パケットに関する詳細情報と、パケットがセキュリティアプライアンスでどのように処理されるかを示します。コンフィギュレーションからのコマンドによってパケットがドロップされなかった場合、packet-tracerコマンドは読みやすい方法で原因に関する情報を提供します。この機能を使用すると、ACLの暗黙の拒否が有効になっていないかどうかを確認できます。次の例は、暗黙のdenyがバイパスされることを示しています(result = ALLOW)。

```
<output truncated>
...
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x1a09d350, priority=1, domain=permit, deny=false
    hits=1144595557, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0000.0000.0000

<output truncated>
```

この脆弱性は、Cisco Bug ID CSCsq91277 (登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2009-1160が割り当てられています。

回避策

このセキュリティ アドバイザリでは、相互に独立した複数の脆弱性が説明されています。これらの脆弱性およびそれぞれ対応策は互いから独立しています。

VPN認証バイパスの脆弱性

アカウントの上書き機能は、tunnel-group general-attributesコンフィギュレーションモードでoverride-account-disableコマンドを使用して有効にします。回避策として、no override-account-disableコマンドを使用してこの機能を無効にします。

巧妙に細工されたHTTPパケットによるDoS脆弱性

SSL VPN（クライアントレスまたはクライアントベース）用に設定されているか、ASDM管理接続を受け入れているデバイスには脆弱性が存在します。

注： IPSecクライアントはこの脆弱性の影響を受けません。

SSL VPN（クライアントレスまたはクライアントベース）を使用しない場合、管理者はASDM接続が信頼できるホストからのみ許可されていることを確認する必要があります。

セキュリティアプライアンスがASDMのHTTPS接続を受け入れるIPアドレスを特定するには、信頼できるホストアドレスまたはサブネットごとにhttpコマンドを設定します。次の例は、IPアドレス192.168.1.100の信頼できるホストを設定に追加する方法を示しています。

```
hostname(config)# http 192.168.1.100 255.255.255.255
```

巧妙に細工されたTCPパケットによるDoS脆弱性

この脆弱性に対する回避策はありません。

巧妙に細工されたH.323パケットによるDoS脆弱性

H.323インスペクションが不要な場合は、無効にする必要があります。この機能を一時的に無効にすることで、この脆弱性を軽減できます。H.323インスペクションを無効にするには、no inspect h323コマンドを使用します。

SQL*Netパケットの DoS脆弱性

SQL*Netインスペクションが不要な場合は、無効にする必要があります。この機能を一時的に無効にすると、この脆弱性が緩和されます。SQL*Netインスペクションを無効にするには、no inspect sqlnetコマンドを使用します。

アクセスコントロールリスト(ACL)バイパスの脆弱性

回避策として、ACLが設定されているインターフェイスに適用されているaccess-group行を削除し、再度適用します。例：

```
<#root>

ASA(config)#

no access-group acl-inside in interface inside

ASA(config)#
```

```
access-group acl-inside in interface inside
```

前の例では、acl-insideという名前のアクセスグループが削除され、内部インターフェイスに再適用されています。または、そのインターフェイスに適用されるACLの下部に明示的なdeny ip any any行を追加することもできます。例：

```
<#root>

ASA(config)#

access-list 100 deny ip any any
```

前の例では、すべてのIPトラフィックに対する明示的な拒否がaccess-list 100の最後に追加されています。

ネットワーク内のCiscoデバイスに適用可能な他の緩和策については、このアドバイザリに関連するCisco適用対応策速報 (https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20090408-asa)を参照してください。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレード ソリューションを確認してください。

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。

次の表に、各脆弱性に対する最初の修正済みソフトウェアリリースを示します。「Recommended Release」行は、本アドバイザリの公開時点において公開済みであるすべての脆弱性に対する修正を含むリリースを示しています。特定の行で特定のリリースのバージョン（First Fixed Releaseより前）を実行しているデバイスには、脆弱性が存在することが確認されています。シスコでは、表の「Recommended Release」行のリリース、またはそれ以降のリリースにアップグレードすることを推奨しています。

脆弱性	影響を受けるリリース	最初の修正済みバージョン	推奨リリース

アカウント上書き機能を使用した場合のVPN認証バイパスの脆弱性	7.0	脆弱性なし	7.0(8)6
	7.1	7.1(2)82	7.1(2)82
	7.2	7.2(4)27	7.2(4)30
	8.0	8.0(4)25	8.0(4)28
	8.1	8.1(2)15	8.1(2)19
巧妙に細工されたHTTPパケットによるDoS脆弱性	7.0	脆弱性なし	7.0(8)6
	7.1	脆弱性なし	7.1(2)82
	7.2	脆弱性なし	7.2(4)30
	8.0	8.0(4)25	8.0(4)28
	8.1	8.1(2)15	8.1(2)19
巧妙に細工されたTCPパケットによるDoS脆弱性	7.0	7.0(8)6	7.0(8)6
	7.1	7.1(2)82	7.1(2)82
	7.2	7.2(4)30	7.2(4)30
	8.0	8.0(4)28	8.0(4)28
	8.1	8.1(2)19	8.1(2)19

巧妙に細工された H.323パケットによる DoS脆弱性	7.0	7.0(8)6	7.0(8)6
	7.1	7.1(2)82	7.1(2)82
	7.2	7.2(4)26	7.2(4)30
	8.0	8.0(4)24	8.0(4)28
	8.1	8.1(2)14	8.1(2)19
巧妙に細工された SQLパケットによる DoSの脆弱性	7.0	脆弱性なし	7.0(8)6
	7.1	脆弱性なし	7.1(2)82
	7.2	7.2(4)26	7.2(4)30
	8.0	8.0(4)22	8.0(4)28
	8.1	8.1(2)12	8.1(2)19
アクセスコントロール リスト(ACL)バイパス の脆弱性	7.0	7.0(8)1	7.0(8)6
	7.1	7.1(2)74	7.1(2)82
	7.2	7.2(4)9	7.2(4)30
	8.0	8.0(4)5	8.0(4)28
	8.1	脆弱性なし	8.1(2)19

修正済みのCisco ASAソフトウェアは、次の場所からダウンロードできます。

http://www.cisco.com/pcgi-bin/tablebuild.pl/ASAPSIRT

修正済みのCisco PIXソフトウェアは、次の場所からダウンロードできます。

http://www.cisco.com/pcgi-bin/tablebuild.pl/PIXPSIRT

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco PSIRTは、巧妙に細工されたTCPパケットによるDoSの脆弱性に対して、一般に公開されているプルーフオブコンセプト(POC)の不正利用を認識しています。Cisco PSIRTでは、本アドバイザリに記載されている他の脆弱性の不正利用事例とその公表は確認しておりません。

巧妙に細工されたTCPパケットによるDoSの脆弱性は、Verizon BusinessのGregory W. MacPhersonとRobert J. Comboによって発見され、シスコに報告されました。

ACLバイパスの脆弱性は、SecureWorksのJon Ramsey、Jeff Jarmoc、およびFernando Medrano氏によってシスコに報告されました。

Cisco PSIRTは、研究者と協力してセキュリティの脆弱性に関する調査を行う機会を非常に高く評価しており、製品レポートのレビューと支援を行う機会を歓迎しています。

その他の脆弱性はすべて、社内テストおよびお客様のサービスリクエストの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090408-asa

改訂履歴

リビジョン 1.2	2009年4月13日	ソフトウェアテーブルの「巧妙に細工されたHTTPパケットによるDoSの脆弱性」セクションで、推奨リリースを8.1(2)16から8.1(2)19に変更。
リビ	2009年	不正利用事例と公式発表の更新

ジョン 1.1	4月8日	
リビジョン 1.0	2009年 4月8日	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。

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。