Cisco PIXおよびCisco ASAの複数の脆弱性

High

アドバイザリーID : cisco-sa-20081022-asa
初公開日 : 2008-10-22 16:00
バージョン 1.0 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID :

CVE-2008-3815
CVE-2008-3816
CVE-2008-3817

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。このアドバイザリは以下の脆弱性の要点について説明しています。

- Windows NTドメイン認証バイパスの脆弱性
- IPv6のDoS脆弱性
- Cryptoアクセラレータのメモリリークの脆弱性

注：これらの脆弱性は互いに独立しています。ある機器が 1 つの脆弱性の影響を受け、他の脆弱性の影響は受けない場合もあります。

シスコはこれらの脆弱性に対処するソフトウェアアップデートをリリースしています。この中のいくつかの脆弱性には影響を軽減する回避策が存在します。

このアドバイザリは、
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20081022-asa で公開されています。

該当製品

脆弱性のある製品

以下に本アドバザリの各脆弱性の詳細について示します。

Windows NTドメイン認証バイパスの脆弱性

Microsoft Windows NTドメイン認証の問題が原因で、Cisco ASAおよびCisco PIXデバイスがVPN認証バイパスの脆弱性の影響を受けやすい場合があります。Microsoft Windows NTドメイ

ン認証を使用するIPSecまたはSSLベースのリモートアクセスVPNが設定されているCisco ASAまたはCisco PIXセキュリティアプライアンスには、脆弱性が存在する可能性があります。他のタイプの外部認証（LDAP、RADIUS、TACACS+、SDI、またはローカルデータベース）を使用しているデバイスは、この脆弱性の影響を受けません。

次の例は、Cisco ASAでコマンドラインインターフェイス(CLI)を使用してWindows NTドメイン認証を設定する方法を示しています。

```
aaa-server NTAuth protocol nt
 aaa-server NTAuth (inside) host 10.1.1.4
 nt-auth-domain-controller primary1
```

または、デバイスでWindows NTドメイン認証が設定されているかどうかを確認するには、show running-config | include nt-auth-domain-controllerコマンドを発行します。

IPv6のDoS脆弱性

ソフトウェアバージョン7.2(4)9または7.2(4)10を実行し、IPv6用に設定されているCisco ASAおよびCisco PIXセキュリティアプライアンスには、脆弱性が存在する可能性があります。この脆弱性は、IPv4専用に設定されたデバイスには影響しません。

注：IPv6機能はデフォルトでオフになっています。

Cisco ASAおよびCisco PIXセキュリティアプライアンスでは、ipv6 addressインターフェイスコマンドを使用してIPv6を有効にします。デバイスでIPv6が設定されているかどうかを確認するには、show running-config | include ipv6コマンドを使用します。

または、次の例に示すように、特権EXECモードでshow ipv6 interfaceコマンドを使用して、IPv6が設定されているインターフェイスのステータスを表示できます。

```
hostname# show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
dmz [up/up]
    unassigned
```

この例では、outsideインターフェイスとdmzインターフェイスはIPv6用に設定されていません。

Cryptoアクセラレータのメモリリークの脆弱性

Cisco ASAセキュリティアプライアンスでは、巧妙に細工された一連の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可能性があります。このメモリリークは、ハードウェア暗号化アクセラレータの初期化コードで発生します。8.0.xリリースのソフトウェアバージョンを実行しているデバイスには脆弱性が存在します。

注：リリース7.0、7.1、および7.2のソフトウェアバージョンを実行しているCisco ASAアプライアンスには、脆弱性はありません。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せん。

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 リリース 8.0(4) を実行している Cisco ASA セキュリティ アプライアンスを示しています。

```
ASA# show version

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

[...]
```

Cisco Adaptive Security Device Manager（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 ウィンドウの左上にソフトウェアのバージョンが表示されます。

脆弱性を含んでいないことが確認された製品

Cisco Firewall Services Module(FWSM)は、これらの脆弱性の影響を受けません。バージョン6.xを実行しているCisco PIXセキュリティアプライアンスには脆弱性はありません。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。

Windows NTドメイン認証バイパスの脆弱性

Microsoft Windows NTドメイン認証の問題が原因で、Cisco ASAおよびCisco PIXデバイスが

VPN認証バイパスの脆弱性の影響を受けやすい場合があります。IPSecまたはSSLベースのリモートアクセスVPNが設定されているCisco ASAまたはCisco PIXセキュリティアプライアンスには、脆弱性が存在する可能性があります。

注：他のタイプの外部認証（LDAP、RADIUS、TACACS+、SDI、またはローカルデータベース）を使用してIPSecまたはSSLベースのリモートアクセスVPNを設定している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せん。

Cisco ASAセキュリティアプライアンスは、NTLMバージョン1をサポートするMicrosoft Windowsサーバオペレーティングシステム（総称して「NTサーバ」と呼ばれる）をサポートしています。NTドメイン認証は、リモートアクセスVPNに対してのみサポートされます。

この脆弱性は、Cisco Bug ID CSCsu65735 (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-2008-3815が割り当てられています。

IPv6のDoS脆弱性

特別に巧妙に細工されたIPv6パケットによって、Cisco ASAおよびCisco PIXセキュリティアプライアンスのリロードが発生する可能性があります。ソフトウェアバージョン7.2(4)9または7.2(4)10を実行し、IPv6が設定されているデバイスには、脆弱性が存在する可能性があります。この脆弱性は、IPv4専用に設定されたデバイスには影響しません。

注:7.0、7.1、8.0、および8.1リリースのソフトウェアバージョンを実行しているデバイスには、脆弱性はありません。

Cisco ASAまたはCisco PIXセキュリティアプライアンスでIPv6を設定するには、少なくとも各インターフェイスにIPv6リンクローカルアドレスを設定する必要があります。さらに、グローバルアドレスをインターフェイスに追加できます。

注：この脆弱性の影響を引き起こす可能性があるのは、（デバイスを通過せずに）デバイス宛てのパケットのみです。これらのパケットは、IPv6用に設定されたインターフェイス宛てである必要があります。

この脆弱性は、Cisco Bug ID CSCsu11575 (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-2008-3816が割り当てられています。

Cryptoアクセラレータのメモリリークの脆弱性

Cisco ASAセキュリティアプライアンスで、一連のパケットによって引き起こされるメモリリークが発生する場合があります。このメモリリークは、ハードウェア暗号化アクセラレータの初期化コードで発生します。

注：この脆弱性は、（デバイスを通過せずに）デバイス宛てのパケットによってのみ引き起こされます。

次のCisco ASA機能は暗号化アクセラレータが提供するサービスを使用するため、この脆弱性の影響を受ける可能性があります。

- クライアントレス WebVPN、SSL VPN クライアント、および AnyConnect 接続
- ASDM(HTTPS)管理セッション
- ネットワーク アクセスのカットスルー プロキシ
- 暗号化された音声検査の TLS プロキシ
- IP Security(IPsec)リモートアクセスおよびサイト間VPN
- セキュアシェル(SSH)アクセス

この脆弱性は、Cisco Bug ID CSCsj25896 (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-2008-3817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。

Windows NTドメイン認証バイパスの脆弱性

LDAP認証は、この脆弱性の影響を受けません。回避策として、Windows NTドメイン認証の代わりに、リモートアクセスVPNに対して別のタイプの外部認証を有効にすることができます。

注：特定のAAAサーバタイプのサポートの詳細については、次のリンクを参照してください。
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/aaa.html#wp1069492

IPv6のDoS脆弱性

デバイスにIPv6機能を必要としないお客様は、no ipv6 addressインターフェイスサブコマンドを使用してIPv6パケットの処理を無効にし、その危険を排除できます

Cryptoアクセラレータのメモリリークの脆弱性

この脆弱性に対する回避策はありません。

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。

次のリストには、各脆弱性に対する第 1 修正済みソフトウェア リリースが含まれています。

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
Windows NTドメイン認証バイパスの脆弱性	7.0	7.0(8)3
	7.1	7.1(2)78
	7.2	7.2(4)16
	8.0	8.0(4)6
	8.1	8.1(1)13
IPv6のDoS脆弱性	7.0	脆弱性なし
	7.1	脆弱性なし
	7.2	7.2(4)11
	8.0	脆弱性なし
	8.1	脆弱性なし
Cryptoアクセラレータのメモリリークの脆弱性	7.0	脆弱性なし
	7.1	脆弱性なし
	7.2	脆弱性なし

	8.0	8.0(4)
	8.1	8.1(2)

次のメンテナンスソフトウェアリリースは、このセキュリティアドバイザリに記載された脆弱性に対する修正を含む最初のソフトウェアリリースです。

以下よりPIXに関する修正版ソフトウエアのダウンロードが可能です。

http://www.cisco.com/pcgi-bin/tablebuild.pl/pix?psrtdcat20e2

以下よりASAに関する修正版ソフトウエアのダウンロードが可能です。

http://www.cisco.com/pcgi-bin/tablebuild.pl/asa?psrtdcat20e2

「Windows NTドメイン認証バイパスの脆弱性」に関しては、暫定修正済みソフトウェアのみが現在提供されています。回避策を適用する代わりに修正済みバージョンにアップグレードすることを希望するお客様は、次の場所からPIXおよびASAの暫定バージョンをダウンロードできます。

http://www.cisco.com/pcgi-bin/tablebuild.pl/PIXPSIRT?psrtdcat20e2

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

このアドバイザリで説明されている脆弱性の公表や悪用に関する情報は Cisco PSIRT には寄せられていません。

これらの脆弱性は、社内テストおよびテクニカルサポート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-20081022-asa

改訂履歴

リビジョン 1.0	2008年10月22日	初版リリース

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。