Cisco PIXおよびCBACフラグメンテーション攻撃

アドバイザリーID : cisco-sa-19980910-pix-cbac-nifrag
初公開日 : 1998-09-10 15:00
バージョン 1.2 : 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

シスコのPIX Firewallも、シスコのIOS FirewallフィーチャセットのContext-Based Access Control(CBAC)機能も、フラグメント化されたIPパケットを含む特定のDoS攻撃からホストを保護しません。この脆弱性では、ネットワークの「侵入」は許可されません。この脆弱性は、スタティックNetwork Address Translation（NAT；ネットワークアドレス変換）エントリを含む設定、またはNATをまったく使用しない設定で最も深刻です。

この脆弱性は、バージョン4.2(1)までのCisco PIX Firewallソフトウェアと、11.2Pおよび11.3Tまでの Cisco IOSソフトウェアのCBACバージョンに存在し、CBACソフトウェアの最初の12.0リビジョンにも存在します。

Cisco Centri Firewallには、この脆弱性は存在しません。

Cisco IOSソフトウェアの非CBACバージョンで使用可能な拡張アクセスリストなどのステートレスパケットフィルタリング製品には、ステートレス動作に固有の制限があるため、この脆弱性が共通しています。これは、ステートレスフィルタリングの不具合とはみなされません。詳細については、このドキュメントの「ステートレスパケットフィルタ」の項を参照してください。

この脆弱性は、1998年9月16日以降にリリースされる予定のCisco PIX Firewallソフトウェアバージョン4.2(2)で修正されます。この脆弱性は、Cisco IOSソフトウェアリリース12.0(2)および12.0(3)TではCBACに対して修正される予定です。これらのリリースは、それぞれ1998年11月下旬と1999年1月下旬に予定されています。すべてのスケジュールは変更される可能性があります。

シスコやその他のベンダーが提供するパケットフィルタに対するIPフラグメンテーション攻撃の可能性は、非常に長い間広く知られています。ただし、不正利用は増加していないようです。したがって、シスコは、お客様の大多数がこの脆弱性に重大な影響を受けていると考えていません

。ただし、シスコは、実際に攻撃を受けたり、このような攻撃を受ける可能性があると考える特定の理由があるお客様をサポートする用意があります。

このアドバイザリは、
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-19980910-pix-cbac-nifrag で公開されています。

該当製品

このセクションには、該当製品に関する詳細が掲載されています。

脆弱性のある製品

ソフトウェアバージョンが4.2(1)以前のCisco PIX Firewallが該当します。Cisco IOSソフトウェアバージョンの11.2Pおよび11.3T（すべての編集レベル）以前のCBAC機能、ならびに12.0バージョンおよび12.0(1)および12.0(2)T以前の12.0Tバージョンも影響を受けます。

同様の脆弱性は、シスコまたはその他のベンダーのステートレスパケットフィルタリング製品を使用するすべてのユーザに影響を与えます。影響を受けるパケットフィルタは、データグラムのすべてのフラグメントに存在するとは限らないTCPまたはUDPport番号などの情報に基づいてフィルタリングできるフィルタです。この脆弱性は、ステートレスパケットフィルタリング製品の不具合とは見なされません。

非CBACのCisco IOSソフトウェア拡張アクセスリストを使用したパケットフィルタリングは、このカテゴリのステートレスフィルタリングに分類されます。このようなアクセスリストは、Cisco IOSソフトウェアのすべてのバージョンにおいて脆弱です。該当する拡張アクセスリストは、100 ~ 199の番号付きリスト、またはextendedキーワードで作成された名前付きアクセスリストです。1 ~ 99の番号が付けられた非拡張Cisco IOSアクセスリストは、ポート番号でのフィルタリングに対応していないため、この脆弱性の影響を受けません。

脆弱性を含んでいないことが確認された製品

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

このセクションでは、これらの脆弱性に関する詳細情報を提供します。

PIX ファイアウォール

PIXファイアウォールのこの脆弱性には、Cisco Bug ID CSCdk36273が割り当てられています。

注：CCO登録ユーザで、ログインしている場合は、バグの詳細を表示できます。

CSCdk36273を表示する(登録ユーザ専用)

PIXファイアウォールの問題の説明

バージョン4.2(1)までのPIX Firewallソフトウェアは、スタティックまたはダイナミックNATテーブルエントリが存在するホスト宛ての先頭以外のフラグメントを渡します。スタティックNATテーブルエントリはPIX Firewall staticコマンドで作成され、ダイナミックエントリはInsideホストによってOutsideホストとの間でIPトラフィック交換が開始されて作成されます。先頭以外のフラグメントが実際の既存の接続に属しているかどうかはチェックされません。したがって、外部ホストは、2つのホスト間に接続が存在するかどうか、およびコンジットが設定されているかどうかにかかわらず、NATエントリを持つ任意の内部ホストにフラグメントを送信できます。

PIXファイアウォールのための迅速な応答

バージョン4.2(2)では、PIX Firewallの動作が次のように変更されています。

- インターフラグメントの状態は現在保持されています。先頭以外のフラグメントは、対応する先頭フラグメントがファイアウォールの通過を許可されない限り、廃棄されます。対応する先頭フラグメントよりも前に受信された先頭以外のフラグメントは廃棄されます。
  これにより、一致しない先頭以外のフラグメントによってホストリソースが過負荷になる可能性がなくなり、攻撃者は、一致しない先頭フラグメントを使用する攻撃に対して比較的精巧なアドレススプーフィングを行う必要があります。
  この変更は、フラグメントの順序が入れ替わったデータグラムをファイアウォールが廃棄してしまうため、特定の状況では好ましくない影響を及ぼす可能性があります。正当なフラグメントの順序が入れ替わる可能性のある配信は、さまざまな状況で発生します。そのため、新しいソフトウェアをインストールする際には注意が必要です。ただし、シスコは、正当な順序の不正なフラグメント化トラフィック（またはあらゆる種類のフラグメント化トラフィック）がインターネットファイアウォールで一般的であるとは考えていません。
- コンジットのないホストに対して受信されたフラグメントは、それらのフラグメントがアクティブな接続と一致しない限り、廃棄されます。マッチングは、IP送信元と宛先のアドレスおよびプロトコルタイプを使用して実行されます。
- フラグメンテーション状態専用のメモリの量は、PIX Firewall自体に対するサービス拒否攻撃の可能性を減らすために制限されます。フラグメンテーション状態は、最初のフラグメントへの応答でのみ作成され、問題のデータグラムのすべてのフラグメントが処理されるか、タイムアウトが切れるまで保持されます。フラグメンテーション状態のリソースが使い果たされたときに受信された先頭フラグメントは廃棄されます。
  フラグメント状態のメモリが不足しているため、フラグメント化されていないトラフィックが廃棄されることはありません。システムがフラグメント化されたパケットによる攻撃を受けている場合でも、正当なフラグメント化されたトラフィックがある場合でも、ファイアウォールのフラグメント状態リソースの一部を引き続き取得し、正当なフラグメント化されていないトラフィックが妨げられずに流れます。

これらの変更または同等の変更は、バージョン4.2(2)以降のすべてのPIX Firewallソフトウェアバージョンに適用されます。

PIXファイアウォールの修正済みソフトウェアの入手

シスコは、サービス契約のステータスにかかわらず、PIX Firewallのすべてのお客様に4.2(2)ソフトウェアへの無償アップグレードを提供しています。アップグレードは、4.2(2)ソフトウェアのリリース後すぐに利用可能になります。

ソフトウェアがリリースされたら、サービス契約を結んでいるお客様は、シスコのWorldwide Webサイトからソフトウェアをダウンロードできます。

サービス契約をご利用でないお客様は、Cisco TACに連絡してアップグレードを入手してください。TAC の連絡先は次のとおりです。

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

無料アップグレードの資格として、この通知の URL をご用意ください。契約を結んでいないお客様向けの無料アップグレードは TAC 経由でご要求いただく必要があります。ソフトウェア アップグレードに関して、「psirt@cisco.com」または「security-alert@cisco.com」にお問い合せいただくことはご遠慮ください。

新しいソフトウェアのインストールと同様に、バージョン4.2(2)へのアップグレードを計画しているPIX Firewallのお客様は、アップグレードを開始する前に、リリースノートやその他の関連ドキュメントを注意深く読む必要があります。

PIXファイアウォールのための長期計画

シスコでは、フラグメンテーションに関連する脆弱性を解消するために、PIX Firewallのフラグメント処理にさらに変更を加える可能性を評価しています。さらに変更を加えると、比較的大きな特性を持つ可能性が高いため、リリース4.2以降のPIX Firewallリリースで変更が発生する可能性があります。

PIXファイアウォールのための回避策

この脆弱性に対する直接的な回避策はありませんが、スタティックNAT エントリへの依存を回避することで、問題の発生を減らすことができます。ダイナミックNATをアクティブに使用しているホストは、修正済みソフトウェアがインストールされるまで、ある程度の脆弱性が残ります。ただし、動的に割り当てられたアドレスに対して脆弱性を悪用することは、静的に割り当てられたアドレスに対して脆弱性を悪用するよりも困難です。ダイナミックNATを介して脆弱性を不正利用するには、攻撃者は任意の時点でどのダイナミックアドレスがアクティブで、どのホストにそれらのアクティブなアドレスが対応しているかを判断するために追加の作業を行う必要があります。

CBAC (Cisco IOS Firewall Feature Set) 詳細

CBAC機能のこの脆弱性には、Cisco Bug ID CSCdk41516が割り当てられています。

注：CCO登録ユーザで、ログインしている場合は、バグの詳細を表示できます。

CSCdk41516を表示する(登録ユーザ専用)

CBAC の問題の説明

Cisco IOS CBAC機能は、11.2Pと11.3Tを含む11.2と11.3ベースのすべてのバージョンまで、および12.0(1)と12.0(2)Tを含む12.0ベースのバージョンまで、先頭以外のIPフラグメントのフィルタリングを行いません。CBAC機能は、拡張IPアクセスリストを動的に変更することによって、フィルタリングの大部分を実行します。また、すべてのCisco IOS拡張アクセスリストと同様に、CBACによって変更されたアクセスリストは、常に先頭以外のフラグメントを通過させます。

CBAC のための迅速な応答

CBAC機能の動作に次の変更が加えられ、現在バージョン12.0(2)および12.0(3)Tを対象としています。

- インターフラグメント状態は保持されます。先頭以外のフラグメントは、対応する先頭フラグメントがファイアウォールの通過を許可されない限り、廃棄されます。対応する先頭フラグメントよりも前に受信された先頭以外のフラグメントは廃棄されます。
  これは、ip inspect設定コマンドで設定されたCBACによって処理されるパケットだけに適用されます。CBACによって検査されないルータトラフィックには、そのトラフィックがアクセスリストでフィルタリングされた場合でも、フラグメンテーション状態チェックは適用されません。
  この変更により、一致しない先頭以外のフラグメントによってホストリソースが過負荷になる可能性がなくなり、攻撃者は、一致しない先頭フラグメントを使用する攻撃に対して比較的精巧なアドレススプーフィングを使用する必要があります。
  この変更は、フラグメントが順不同で到着したパケットをファイアウォールが廃棄する結果になるため、特定の状況では望ましくない影響を及ぼす可能性があります。正当なフラグメントの順序が入れ替わる可能性のある配信は、さまざまな状況で発生します。Cisco IOSソフトウェアが稼働するルータは非常に多様なネットワークで使用されており、またCBAC機能は内部ネットワークの各部分を互いに隔離するために頻繁に使用されるため、新しい動作はデフォルトでは有効になっていません。フラグメントチェックは、ip inspect name inspect-name fragment設定コマンドを使用して明示的に有効にする必要があります。シスコでは、特に必要な特別な状況がない限り、CBACがインターネットファイアウォールとして使用されている場合は常にこのコマンドを使用することを推奨しています。シスコでは、インターネットファイアウォールでは正規の不正なフラグメントはまれであると考えています。
- フラグメンテーション状態専用のメモリの量は、ファイアウォールルータ自体に対するサービス拒否攻撃の可能性を減らすために制限されます。フラグメンテーション状態は、最初のフラグメントへの応答でのみ作成され、問題のデータグラムのすべてのフラグメントが処理

されるか、タイムアウトが切れるまで保持されます。フラグメンテーション状態のリソースが使い果たされたときに受信された先頭フラグメントは廃棄されます。
フラグメント状態のメモリが不足しているため、フラグメント化されていないトラフィックが廃棄されることはありません。システムがフラグメント化されたパケットによる攻撃を受けている場合でも、正当なフラグメント化されたトラフィックがある場合でも、ファイアウォールのフラグメント状態リソースの一部を引き続き取得し、正当なフラグメント化されていないトラフィックが妨げられずに流れます。

- フラグメント長の正当性がチェックされ、ポート番号上書き攻撃を回避するためにフラグメントオフセットがチェックされます。このオフセットチェックは、CBACがアクセスリストなしで使用されている特殊な設定に対して、拡張アクセスリストによってすでに適用されているチェックを複製します。

これらの変更または同等の変更は、Cisco IOSファイアウォール機能セットの今後のすべてのバージョンに適用されます。

CBAC の修正済みソフトウェアの入手

シスコは、サービス契約のステータスに関係なく、Cisco IOS Firewallフィーチャセットを購入されたすべてのお客様に無償アップグレードを提供しています。ステートレスパケットフィルタリングには不具合がないため、この無償のアップグレードプログラムは、ファイアウォール以外のCisco IOSのみを購入されたお客様には適用されません。

更新されたソフトウェアがリリースされたら、サービス契約を結んでいるお客様は、通常のチャネルでCisco IOSソフトウェアアップデートを入手する必要があります。シスコまたはほとんどのリセラーから購入したサービス契約をお持ちのお客様は、シスコのワールドワイドWebサイトからアップデートをダウンロードできます。

サービス契約をご利用でないお客様は、Cisco TACに連絡してアップグレードを入手してください。TAC の連絡先は次のとおりです。

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

無料アップグレードの資格として、この通知の URL をご用意ください。契約を結んでいないお客様向けの無料アップグレードは TAC 経由でご要求いただく必要があります。ソフトウェア アップグレードに関して、「psirt@cisco.com」または「security-alert@cisco.com」にお問い合せいただくことはご遠慮ください。

新しいソフトウェアのインストールと同様に、アップグレードを計画しているお客様は、アップグレードを開始する前に、リリースノートやその他の関連ドキュメントを注意深く読む必要があります。また、使用しているハードウェアで新しいバージョンのCisco IOSソフトウェアがサポートされていること、特に十分なDRAMが使用できることを確認することが重要です。

CBAC のための長期計画

シスコでは、フラグメンテーションに関連する脆弱性を解消するために、Cisco IOS Firewall機能セットのフラグメント処理にさらに変更を加える可能性を評価しています。さらに変更を加えると、比較的大きな特性を持つことになるため、リリース12.0以降のCisco IOSソフトウェアリリースに含まれる可能性があります。

CBAC のための回避策

この脆弱性に固有のCBAC回避策はありません。ただし、ダイナミックNATを使用することで、お客様のリスクを軽減できる可能性があります。また、非拡張IPアクセスリストはIPフラグメントをフィルタリングできるため、一部の設定で潜在的な攻撃を制御するのに役立つ場合があります。

ステートレスパケットフィルタ

Cisco IOSソフトウェアの従来のアクセスリストなどのステートレスIPパケットフィルタは、特定のパケットに対して、そのパケット内の情報のみに基づいてすべての転送を決定する必要があります。フィルタリングがTCPやUDPのポート番号などの基準に基づいている場合、必要な情報は通常、フラグメント化されたデータグラムの先頭フラグメント内にのみ存在します。したがって、先頭以外のフラグメントが、禁止されているデータグラムの一部なのか、許可されているデータグラムの一部なのかを判断することは不可能です。したがって、このような基準を使用するステートレスパケットフィルタは、先頭以外のすべてのフラグメント、またはほぼ全てのフラグメントを通過させる必要があります。このようなフィルタは、禁止されたデータグラムの完全な配信を防ぐために、先頭フラグメントのブロックに依存します。このため、このNoticeで説明されているフラグメンテーションDoS攻撃に対する脆弱性が存在します。

Cisco IOSソフトウェアの拡張アクセスリストは、TCPおよびUDPポート番号に加え、ICMPパケットタイプに基づいてフィルタリングを行うことができるため、脆弱性のあるカテゴリに分類されます。Cisco IOSソフトウェア拡張アクセスリストは、フラグメント化されたIPデータグラムの先頭以外のフラグメントを渡します。

ポート番号などの情報を使用しないステートレスパケットフィルタでも、データグラムのすべてのフラグメントに情報が存在するため、この脆弱性の影響を受けません。Cisco IOSソフトウェアの非拡張アクセスリストがポート番号で一致しない。したがって、先頭フラグメントだけでなく、先頭以外のフラグメントもフィルタリングできます（また、フィルタリングできます）。

フラグメンテーション攻撃に対する脆弱性は、ステートレスIPパケットフィルタリングのよく知られた、そして主に固有の制限です。シスコでは、この問題をステートレスパケットフィルタリング製品の不具合とは考えておらず、これらの製品に対する即時対応は計画していません。シスコでは、将来的にステートレスフィルタリング製品のフラグメント処理を改善する可能性がありますが、フィルタリング基準にポート番号が含まれている場合、攻撃者が特定のステートレスパケットフィルタを通過するフラグメントを作成することを完全に防ぐ方法はありません。したが

って、このようなフィルタを使用して、フラグメンテーションベースのDoS攻撃を完全に回避する方法はありません。

回避策

回避策については、「詳細」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。

ソフトウェアバージョンと修正の詳細については、「詳細」を参照してください。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

この脆弱性は、シスコおよびその他のベンダーが提供する、ステートフルおよびステートレスの両方の多数のパケットフィルタリングデバイスに共通するものです。この脆弱性は、ルータベースのステートレスパケットフィルタリングでよく知られており、ステートレスフィルタの使用時に攻撃者によって悪用されることがあります。PIX FirewallやCBACなどのステートフルフィルタに対する不正利用は、適宜に発生することが想定される場合があります。

この脆弱性は、さまざまな種類のパケットのフラッドによって「偶然」に悪用される可能性があるため、攻撃者が意図的にこの特定の問題を標的にすることを決定した場合だけでなく、攻撃者が自身でも標的を損傷しているメカニズムを十分に理解していない場合にも、いくつかの問題が発生する可能性があります。

シスコでは、この脆弱性に特有の組織的かつ体系的な不正利用は確認していません。しかし、これを実行する可能性のあるフラッディング攻撃は、インターネット上で一般的に発生するイベントと考えられます。このようなフラッディング攻撃は、標的となるネットワークに対して広範な否定的応答を引き起こします。この脆弱性は、そうした否定的応答の1つです。

この脆弱性を不正利用できるフラッディングツールが広く利用されています。この脆弱性を選択的に悪用するように設計された特殊な目的のツールは比較的まれのように思われますが、シスコではそのようなツールの徹底的な検索は行っていません。このようなツールは、比較的高度な知

識を持つネットワークプログラマが簡単に作成できます。

この脆弱性は、1998年8月下旬に開始されたBUGTRAQメーリングリストでCisco PIX Firewallに関する具体的な説明とともに公開されています。この脆弱性はパケットフィルタ全般に適用されるため、他の公開フォーラムでも多くの議論がなされてきました。シスコ製品に特に適用される場合、この脆弱性に関する公開の議論があったものと考えるのが妥当です。この脆弱性は、コンピュータセキュリティコミュニティと「クラッカー」コミュニティの両方で広く知られていると考える必要があります。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-19980910-pix-cbac-nifrag

改訂履歴

リビジョン 1.2	1998年9月11日	再びPIXのリリース日を修正
リビジョン 1.1	1998年9月11日	実際の初期リリースバージョン、修正済みPIXリリース日
リビジョン 1.0	1998年9月10日	最初にリリースされたバージョン

利用規約

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。