Cisco IOS DFSアクセスリストの漏洩

アドバイザリーID : cisco-sa-19981105-ios-dfs-acl
初公開日 : 1998-11-05 16:00
バージョン 1.3 : 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

特定のルータ用の特定のCisco IOSソフトウェアバージョンのエラーにより、IPデータグラムのフィルタリングにアクセスリストが適用されている場合でも、これらのデータグラムがネットワークインターフェイスに出力される可能性があります。これは、Cisco 7xxxファミリのルータにのみ適用され、これらのルータが分散型ファストスイッチング(DFS)用に設定されている場合にのみ適用されます。

Cisco Bug ID CSCdk35564およびCSCdk43862が割り当てられた、2つの独立した脆弱性があります。各脆弱性は、DFS構成の特定のサブセットにのみ影響します。該当する構成は非常に一般的なものとは考えられていませんが、非常にまれなものでもありません。影響を受ける設定の詳細については、このドキュメントの「影響を受けるユーザ」セクションを参照してください。

これらの脆弱性により、ユーザはお客様のネットワークの許可されていない部分にパケットを送信できる可能性があります。これにより、お客様のコンピュータシステムやデータへの不正アクセスやその他の攻撃が許可される可能性があります。シスコでは、これらの脆弱性が攻撃者によって実際に悪用されたインシデントを把握していません。

いずれの脆弱性も、70xxまたは75xxシリーズのルータ以外のシスコ製品には影響しません。70xxルータのうち、オプションのroute-switch processor（RSP；ルートスイッチプロセッサ）カードが装着されているルータだけが該当します。追加の設定条件が適用されます。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-19981105-ios-dfs-acl 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

これらの脆弱性は、Cisco 7xxxルータファミリにのみ該当します。Cisco 7xxxファミリは、主にインターネットサービスプロバイダーや大規模な企業ネットワークで使用される、ラックマウント型の大型バックボーンルータです。

Cisco 75xxルータは、両方の脆弱性の影響を受けます。Cisco 70xxルータは、RSPカードが取り付けられている場合にのみ該当します。Cisco 72xxルータは、いずれの脆弱性の影響も受けません。このNoticeの以前のバージョンでは72xxルータについて誤って言及されていましたが、該当するハードウェアの設定は72xxプラットフォームでは行うことができず、DFSは72xxルータでは設定できません。

CSCdk35564 影響を受ける設定

CSCdk35564は、11.1CCおよび11.1CTリリースの不具合です。11.1CCおよび11.1CT以外のCisco IOSソフトウェアバージョンを実行するルータは、CSCdk35564の影響を受けません。Cisco 75xxルータは該当します。Cisco 70xxルータは、該当するハードウェアとソフトウェアの組み合わせではサポートされません。

注：CCOの登録ユーザとしてログインしている場合は、バグ情報を表示できます。

- CSCdk35564の表示

CSCdk35564の影響を受けるには、DFSが有効なインターフェイスからDFSが有効でないインターフェイスにトラフィックを切り替えるようにルータを設定する必要があります。これは、ルータにVersatile Interface Processor(VIP)インターフェイスカードと非VIPインターフェイスカードの両方が搭載されている場合に最も一般的に発生します。DFSはVIPインターフェイスでのみサポートされているため、VIPから非VIPインターフェイスへのトラフィックはDFSから非DFSに送信される可能性があります。

CSCdk43862 影響を受ける設定

CSCdk43862は、Cisco 70xxおよび75xxシリーズ上のCisco IOSソフトウェアのバージョン11.1、11.2、および11.3に影響を与えます。詳細については、このドキュメントで後述する表を参照してください。

注：CCOの登録ユーザとしてログインしている場合は、バグ情報を表示できます。

- CSCdk43862の表示

この脆弱性を不正利用するには、DFSが有効になっている入力インターフェイスから、物理出力インターフェイスの論理サブインターフェイスにトラフィックをスイッチングするようにルータを設定する必要があります。出力インターフェイスでDFSが有効になっているかどうかは関係ありません。出力インターフェイスの重要な問題は、サブインターフェイスが使用されているかどうか、およびサブインターフェイスへの出力トラフィックがフィルタリングされてい

るかどうかです。

脆弱性を含んでいないことが確認された製品

脆弱性はそれぞれ異なり、異なる条件下で現れますが、どちらもDFSに関係しています。DFSはシスコ製品ではデフォルトで有効になっていないため、手動で設定する必要があります。ip route-cache distributedコマンドがルータコンフィギュレーションファイルに表示されない場合、どちらの脆弱性の影響も受けません。

特に、プロセススイッチング(no ip route-cache)、通常のファストスイッチング(ip route-cache)、最適スイッチング(ip route-cache optimum)、およびCEFまたはdCEFスイッチング(ip route-cache cef、ip cef distributed switch)は影響を受けません。フロースイッチングはファストスイッチングの一種と見なされ、分散モードでのみ影響を受けます。フロースイッチングとアクセスリストの間のインタラクションにより、DFSとともにフロースイッチングを有効にした場合の両方の脆弱性の影響が軽減されますが、この影響が排除されるわけではありません。

ルータのすべてのインターフェイスでDFSが有効になっている場合、CSCdk35564の影響は受けません。ルータのどのインターフェイスでもDFSが有効になっていない場合は、この問題には該当しません。ip access-groupコマンドを使用して非DFSインターフェイスの発信トラフィックをフィルタリングしない場合、この問題には該当しません。

サブインターフェイスは、物理インターフェイス上のトラフィックのサブセットに関連付けられた擬似インターフェイスです。たとえば、物理フレームリレーインターフェイスには、各フレームリレーPVCに関連付けられたサブインターフェイスがある場合があります。サブインターフェイスはデフォルトでは存在せず、ユーザ設定の一部として作成されます。「Serial 0/1.1」のように、サブインターフェイス番号には常にピリオドが含まれます。コンフィギュレーションファイルにそのような「ドット付き」のインターフェイス番号が含まれていない場合は、脆弱ではありません。

ip access-groupコマンドを使用して出力アクセスリストフィルタリングをサブインターフェイスに適用しない場合、この脆弱性は存在しません。

CSCdk43862により、物理インターフェイスの1つのサブインターフェイスに適用されるアクセスリストが、別のサブインターフェイス宛てのトラフィックに誤って使用されます。同じアクセスリストを使用して、任意の物理インターフェイスのすべてのサブインターフェイスで発信トラフィックをフィルタリングする場合、この脆弱性は存在しません。

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

CSCdk43862に重複するレポートがCSCdk43696ります。この不具合を参照するには、Bug ID CSCdk43862を使用する必要があります。

回避策

これらの脆弱性は、ネットワークインターフェイスでDFSを無効にすることで回避できます(no ip route-cache distributedを使用)。DFSの目的は、ルータのプライマリCPUからVIPカード上のCPUに計算負荷を転送することであり、そのためDFSを無効にするとプライマリCPUが過負荷状態になる可能性があることに注意してください。この回避策を使用する前に、トラフィック負荷とCPU使用率を評価してください。

ルータ内のすべてのインターフェイスがDFSに対応しているが、何らかの理由でDFSが一部のインターフェイスでのみ有効になっている場合は、すべてのインターフェイスでDFSを有効にすることでCSCdk35564を回避できる可能性があります。これはCSCdk43862には影響しません。

物理インタCSCdk43862フェイスのすべてのサブインターフェイスで同じ出力アクセスリストを使用するように再設定することで、問題を回避できる場合があります。

もう1つの回避策として、ルータのアクセスリスト構造を再設計して、影響を受けるインターフェイスに出力アクセスリストが必要になるのを回避する方法があります。

修正済みソフトウェア

次の表に、CSCdk35564とCSCdk43862の両方の該当するCisco IOSソフトウェアバージョンの概要と、修正されたバージョンを示します。この表を使用するには、表の最初の列で、現在実行中のソフトウェアリリース(ルータのshow versionコマンドで使用可能)を調べます。表の他の列には、メジャーリリースで修正されているCisco IOSソフトウェアバージョンと、シスコがインストールを推奨するバージョンが示されています。

次の表に、暫定バージョンと通常リリースされているバージョンの両方を示します。暫定バージョンは、通常のリリース版と比較して、受け取るテストが大幅に少なく、品質も一般に確実性に欠けています。シスコでは、可能な限り定期的にリリースされるソフトウェアをインストールすることを推奨しています。暫定バージョンは参照用として、また適切な正規リリースのバージョンが利用可能になる前にアップグレードする必要があるお客様の便宜のためにリストされています。

通常どおり、メジャーリリースの1つの通常のリリースバージョンに適用される修正は、そのメジャーリリースの以降のすべてのバージョンも修正されることを意味します。たとえば、11.2(17)は固定されているため、11.2(18)以降も固定されています。

この表は、該当するすべてのCiscoルータでサポートされているすべてのソフトウェアを網羅するように設計されています。75xxルータまたはRSPプロセッサを搭載した70xxルータで分散型ファーストスイッチングを実行し、表に記載されていない11.1、11.2、または11.3リリースを使用している場合は、Cisco TACに連絡してサポートを受けてください。

Cisco IOSメジ	初期CSCdk35564修正	初期CSCdk43862修正	7xxx DFSユーザ

ャーリリース（7xxxリリースのみ記載）	暫定（最小限のテスト、緊急アップグレードのみ）	通常（日付は変更されることがあります）	暫定（最小限のテスト、緊急アップデートのみ）	通常（日付は変更されることがあります）	ーのアップグレードパス
11.0以前、すべてのバリアント	影響なし	影響なし	影響なし	影響なし	影響なし
11.1	影響なし	影響なし	-	-	11.1CAに移動
11.1 CA（コアED）	影響なし	影響なし	11.1(22)CA	11.1(22)CA	11.1(22)CA以降
11.1CC（CEF版）	11.1(21.2)CC	11.1(21)CC1 11.1(22)CC	11.1(21.2)CC	11.1(21)CC1 11.1(22)CC	11.1(21)CC1、 11.1(22)CC以降
11.1CT（タグスイッチED）	11.1(21.2)CT	11.1(22)CT	11.1(21.2)CT	11.1(22)CT	11.1(22)CT以降
11.2	影響なし	影響なし	11.2（16.1）	11.2(17)、1999年1月予定	11.2(17)以降、 11.2(16.1)または 11.3(11.2(17)のスケジュールが受け入れられない場合)
11.2F	影響なし	影響なし	-	-	11.3に進む
11.2P（プラットフォームED）	影響なし	影響なし	11.2(16.1)P	11.2(17)P、 1999年1月予定	11.2(17)P以降、 11.2(16.1)Pまたは 11.3(11.2(17)Pスケジュールが許容されない場合)

11.2BC(CIP ED)	影響なし	影響なし	11.2(16.1)BC	11.2(17)BC、1999年1月予定	11.2(17)BC以降。11.2(17)BCのスケジュールが許容されない場合は11.2(16.1)BC。
11.3	影響なし	影響なし	11.3（6.2）	11.3(7)、1998年11月予定	11.3(7) 以降
11.3T	影響なし	影響なし	11.3(6.2)T	11.3(7)T（1998年11月予定）	11.3(7)T以降
11.3NA（音声ED）	影響なし	影響なし	11.3(6.2)NA	11.3(7)NA、1998年12月予定	11.3(7)NA以降。11.3(7)NAのスケジュールが許容範囲外の場合は11.3(6.2)NA。
11.3(2)XA	影響なし	影響なし	-	-	11.3(7) 以降
12.0(1)以降、すべてのバリアント	影響なし	影響なし	影響なし	影響なし	影響なし

ポートアダプタのサポートが制限されているため、多くのお客様が11.1メインラインソフトウェアでDFSを使用しているとはシスコでは考えていません。機能と安定性の両方の理由から、11.1CAを推奨します。

11.1(21)CC1リリースは11.1CCの特別なリリースです。11.1CCリリースシーケンスは、11.1(21)CC ~ 11.1(21)CC1、さらに11.1(22)CCまで続きます。

11.3(2)XAは、11.3(2)に基づく特別な1回限りのリリースです。11.3(2)XAの機能は11.3(3)リリースに組み込まれています。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

シスコは、この通知の日付より前に、これらの脆弱性に関する公表または議論を行うことはできません。

シスCSCdk35564のお客様によるインストールシステムテストで発見されました。シスコの社内テストでCSCdk43862が発見されました。

これらの脆弱性の性質上、攻撃者がこれらの脆弱性を直接悪用することはほとんどありません。ほとんどの場合、攻撃者は、管理者がアクセスを拒否したと考えていたネットワークリソースへのアクセスを自分自身に気付くだけです。シスコには、この脆弱性が原因で悪意のある攻撃が成功したという実際の報告はなく、また「脆弱な」状態を意図的に作ろうとしている人物の報告もありません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-19981105-ios-dfs-acl

改訂履歴

リビジョン 1.3	1998年11月5日	初回公開リリース

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。