Cisco 6000/6500/7600 Crafted Layer 2 Frame Vulnerability

severity

アドバイザリーID : cisco-sa-20040203-cat6k

初公開日 : 2004-02-03 16:00

バージョン 1.0 : 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

レイヤ3パケット（IP、IPXなど）をカプセル化しているレイヤ2フレーム(Open System Interconnection Reference Modelで定義)が原因で、FlexWANまたはOptical Services Module（OSM；オプティカルサービスモジュール）を搭載した、または12.1(8b)E14を実行するMultilayer Switch Feature Card 2（MSFC2；マルチレイヤスイッチフィーチャカード2）を搭載したCisco 6000/600/700シリーズシステム0が、または0000、リセット00000、または00000000000000000000000000000000カプセル化されたレイヤ3パケットの長さ。

この脆弱性が繰り返し悪用されると、サービス拒否が発生する可能性があります。

この脆弱性は、Cisco Bug ID CSCdy15598およびCSCeb56052で対処されています。

回避策はありません。この脆弱性に対処するには、ソフトウェアのアップグレードが必要です。

このアドバイザリは、シスコのワールドワイドWebサイト https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040203-cat6kで公開されます。

該当製品

脆弱性のある製品

MSFC2とFlexWANまたはOSMモジュールを搭載したCisco 6000/6500/7600シリーズシステムが該当します。

12.1(8b)E14を実行しているMSFC2を搭載したCisco 6000/6500/7600シリーズシステムは、FlexWANまたはOSMモジュールがない場合でも該当します。

Supervisor 720を搭載したCisco 6000/6500/7600シリーズシステムは、この脆弱性の影響を受けません。

該当するシステムでは、Cisco IOSシステムソフトウェアまたはCatOSシステムソフトウェアが稼働している可能性があります。

show moduleコマンドを使用すると、システムにFlexWANモジュールまたはOSMモジュールがあるかどうかを確認できます。FlexWANモジュールの部品番号はWS-X6182-2PAです。OSMモジュールの部品番号にはOSMが含まれています。

システムで使用されているMSFCのタイプの判別についての詳細は、http://www.cisco.com/warp/public/473/96.htmlを参照してください。

この脆弱性は、指定されたハードウェアまたはソフトウェア設定を持つCisco 6000/6500/7600シリーズシステムにのみ影響します。他のすべてのシステムは、該当するバージョンのIOSを実行する可能性がありますが、この脆弱性の影響を受けません。

Cisco 製品で稼働しているソフトウェアを確認するには、デバイスにログインし、show version コマンドを発行してシステム バナーを表示します。Cisco IOSソフトウェアは、「Internetwork Operating System Software」または単に「IOS Â®」として識別されます。出力の次の行では、イメージ名がカッコで囲まれて表示され、その後に「Version」とIOSリリース名が続きます。その他の Cisco デバイスには show version コマンドがないか、異なる出力が返されます。

次の例は、IOSリリース12.1(11b) E1を実行し、インストールされているイメージ名がC6MSFC2-JSV-Mであるシスコ製品を示しています。

Cisco Internetwork Operating System(IOS)ソフトウェアIOS(tm)

MSFC2ソフトウェア(C6MSFC2-JSV-M)、バージョン12.1(11b)E1、EARLY DEPLOYMENT RELEASE SOFTWARE(fc1)

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

プロトコルに依存しないレイヤ3パケット（IP、IPXなど）をカプセル化しているレイヤ2フレームは、MSFC2を搭載したCisco 6000/6500/7600シリーズシステムをフリーズまたはリセットさせる可能性があります。レイヤ2フレームの実際の長さは、カプセル化されたレイヤ3パケットの長

さと一致しない必要があります。

Cisco 6000/6500/7600シリーズシステムによってルーティングされるレイヤ3パケットは、パケットが特別に細工されたレイヤ2フレームにカプセル化されている場合、この脆弱性を引き起こす可能性があります。この脆弱性を引き起こすには、巧妙に細工されたパケットを脆弱なシステムでソフトウェアでスイッチングする必要があります。ハードウェアでスイッチングされるパケットは、この脆弱性を引き起こしません。

このようなフレームはローカルネットワークセグメントからのみ送信できますが、この脆弱性をリモートで引き起こす可能性がある場合があります。リモートで悪用するには、巧妙に細工されたレイヤ2フレームが、送信元と宛先の間のすべての中間レイヤ3デバイスをクリップされずに通過する必要があります。送信元から宛先までのパス上の単一のレイヤ3デバイスが、巧妙に細工されたレイヤ2フレームをクリップしている場合でも、リモートで悪用されることはありません。Cisco 6000/6500/7600シリーズだけが、このような巧妙に細工されたフレームを修正せずに転送します。

この脆弱性は、Cisco Bug ID CSCdy15598およびCSCeb56052で対処されています。

- **CSCdy15598**:MSFCおよびFlexWANまたはOSMモジュールを搭載したCisco 6000/6500/7600シリーズに影響します。FlexWANまたはOSMを搭載していないシステムは、この不具合の影響を受けません。
- **CSCeb56052**:MSFCモジュールを搭載したCisco 6000/6500/7600シリーズに影響します。この不具合の影響を受けるのは12.1(8b)E14のみで、他のソフトウェアバージョンは影響を受けません。FlexWANまたはOSMを搭載していないシステムでも、12.1(8b)E14を実行している場合は、この不具合の影響を受けます。

これらの不具合の詳細を調べるには、Bug Toolkit(登録ユーザ専用)を使用できます。

回避策

回避策はありません。この脆弱性は、該当するシステムを再設定することによって軽減することはできません。ソフトウェアのアップグレードが必要です。

修正済みソフトウェア

Cisco IOS ソフトウェア

次の表の各行は、リリーストレインと、対象のプラットフォームまたは製品を示しています。特定のリリーストレインに脆弱性が存在する場合は、修正を含む最初のリリースと、各リリースの提供予定日が「リビルド」、「暫定」、および「メンテナンス」の各列に表示されます。特定の列のリリースより前（最も古い固定リリースより前）の特定のトレインのリリースを実行しているデバイスは脆弱であることが知られており、少なくとも示されたリリースまたは新しいバージョン（最も古い固定リリースのラベルより大きい）にアップグレードする必要があります。

リリースを選択するときは、次の定義を念頭においてください。

- Rebuildâ：同トレイン前のメンテナンスまたはメジャーリリースから構築され、特定の脆弱性に対する修正が含まれています。受け取る検査は少ないですが、修理に必要な最小限の変更しか含まれていません。シスコでは、この脆弱性に対処するために複数のメインラインとレインのリビルドを提供していますが、最新のメンテナンスリリースのみをメインラインとレインで実行することを強く推奨します。
- 内部：メンテンスリース間の定期的な間隔で構築され、受け取るテストが少なくなります。[Interims]は、この脆弱性に対処する適切なリリースが他にない場合にのみ選択し、暫定イメージは次の利用可能なメンテナンスリリースにできるだけ早くアップグレードする必要があります。暫定リリースは製品としては提供されず、通常は、Cisco Technical Assistance Center（TAC）によって事前に手配されない限り、CCO からダウンロードできません。
- Maintenanceâテブルの特定の行にあるラベルの最も頻繁にテストされ、強く推奨されるリリース。

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。情報が明確でない場合は、この表の次のセクションに示すように、Cisco TACに連絡して支援を求めてください。

トレイン	修正済みリリースの入手可能性		
	リビルド	Interim	メンテナンス
12.1E	12.1(8b)E15	12.1(13.5)E	12.1(19)E
	12.1(11b)E14	â	â
	12.1(13)E1	â	â
12.2SY	â	â	12.2(14)SY
12.2ZA	â	â	12.2(14)ZA

Cisco CatOSソフトウェア

Cisco CatOSは、この脆弱性の影響を受けません。CatOSシステムソフトウェアの場合は、Cisco CatOSソフトウェアのバージョンを変更する必要はありません。

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040203-cat6k

改訂履歴

リビジョン 1.0	2004年2月3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。