複数の巧妙に細工されたIPv6パケットによるリロード

アドバイザリーID : cisco-sa-20050126-ipv6 CVE-2005-0195
初公開日 : 2005-01-26 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

Cisco Internetwork Operating System(IOS)ソフトウェアは、デバイスがIPv6トラフィックを処理するように設定されている場合、巧妙に細工されたIPv6パケットによるサービス拒否(DoS)攻撃に対して脆弱です。この脆弱性を悪用するには、巧妙に細工された複数のパケットをデバイスに送信する必要があり、不正利用に成功するとリロードが発生する可能性があります。

シスコはこの脆弱性に対処する無償ソフトウェアを提供しています。

影響を緩和するための回避策があります。

この問題はCERT/CC VU#472582で追跡されています。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050126-ipv6で確認できます。

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

この脆弱性に該当するのは、IOSが稼働し、IPv6が設定されているシスコデバイスだけです。ルータは、show ipv6 interfaceコマンドを使用して、すべてのIPv6対応インターフェイスを表示します。

システムでIPv6が無効になっているかサポートされていない場合は、空の出力またはエラーメッセージが表示されます。この場合、システムは脆弱ではありません。

IPv6が設定されたシステムでのshow ipv6 interfaceコマンドの出力例を次に示します。

<#root>

```
  Router#
show ipv6 interface
  Serial1/0 is up, line protocol is up
    IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:D200
    Global unicast address(es):
      2001:1:33::3, subnet is 2001:1:33::/64 [TENTATIVE]
    Joined group address(es):
      FF02::1
      FF02::1:FF00:3
      FF02::1:FF00:D200
    MTU is 1500 bytes
    ICMP error messages limited to one every 100 milliseconds
    ICMP redirects are enabled
    ND DAD is enabled, number of DAD attempts: 1
    ND reachable time is 30000 milliseconds
  Router#
```

物理インターフェイスまたは論理インターフェイスでIPv6が有効になっているルータは、ipv6 unicast-routingがグローバルに無効になっている場合でも、この問題に対して脆弱です。show ipv6 interfaceコマンドを使用すると、任意のインターフェイスでIPv6が有効になっているかどうかを確認できます。

脆弱性を含んでいないことが確認された製品

Cisco IOSを実行していない製品は該当しません。

IPv6インターフェイスが設定されていないCisco IOSの任意のバージョンを実行している製品には、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

IPv6は「Internet Protocol Version 6」であり、現在のバージョンのInternet Protocol, IP Version 4(IPv4)に代わるものとして、Internet Engineering Task Force（IETF；インターネット技術特別調査委員会）によって設計されました。

脆弱性はIPv6パケットの処理に存在し、不正利用されるとシステムのリロードを引き起こす可能性があります。この脆弱性は、物理インターフェイスだけでなく、論理インターフェイス（6to4トンネルを含むトンネル）で受信された巧妙に細工されたパケット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には、巧妙に細工された複数のIPv6パケットを送信する必要があります。このような巧妙に細工されたパケットはリモートで送信できます。

この問題は、Cisco Bug ID CSCed40933(登録ユーザ専用)に記述されています。

回避策

回避策の効果は、製品の組み合わせ、ネットワークトポロジ、トラフィックの動作、組織のミッションなど、お客様の状況によって異なります。該当する製品とリリースは多岐に渡るので、サービス プロバイダーやサポート機関に連絡し、ネットワーク内で使用するのに最も適した回避策を確認してから、実際に配備することを推奨いたします。

ネットワークを移動するトラフィックをブロックするのは往々にして困難ですが、インフラストラクチャ デバイスに送られてはならないトラフィックを識別し、ネットワークの境界でそのトラフィックをブロックすることは可能です。インフラストラクチャアクセスコントロールリスト(ACL)は、ネットワークセキュリティのベストプラクティスと考えられており、ここでの特定の脆弱性の回避策としてだけでなく、優れたネットワークセキュリティへの長期的な付加機能として考慮する必要があります。http://www.cisco.com/warp/public/707/iacl.htmlで入手できる『Protecting Your Core: Infrastructure Protection Access Control Lists』というホワイトペーパーには、インフラストラクチャ保護ACLのガイドラインと推奨される導入方法が記載されています。例外には、インフラストラクチャにアクセスする正当な理由があるデバイス（BGPピア、DNSサーバなど）が含まれます。その他のトラフィックはすべて、どのデバイスでも終端することなくネットワークを通過できる必要があります。

修正済みソフトウェア

メジャー リリース	修正済みリリースの入手可能性		
該当する 12.0 ベースのリリース	リビルド	Interim	メンテナンス
12.0S	12.0(23)S以前のバージョンには脆弱性はありません。		
	12.0(24)S6		

	12.0(25)S3		
	12.0(26)S2		
	12.0(27)S1		
			12.0(28)S
12.0SX	12.0(25)SX8		
12.0SZ	12.0(27)SZ		
該当する 12.2 ベースのリリース	リビルド	Interim	メンテナンス
12.2B	12.2(2)B - 12.2(4)B7 12.2(13)T14以降への移行が必要		
	12.2(4)B8およびFWDを12.3(7)T以降に移行		
12.2BC	12.3(9a)BCに移行		
12.2BX	12.3(7)XI1に移行		
12.2BZ	12.3(7)XI1に移行		
12.2CX	計画はありません。		
12.2CZ	計画はありません。		

12.2EW	12.2(18)EW1		
12.2EWA			12.2(20)EWA
12.2JK	12.2(15)JK2		
12.2MC	12.3(11)Tに移行		
12.2S	12.2(14)S9		
	12.2(18)S5		
	12.2(20)S3		
	12.2(22)S1		
			12.2(25)S
12.2SE	12.2(25)SE		
12.2SU	12.2(14)SU1		
12.2SV	12.2(23)SV		
12.2SW	12.2(23)SW		
12.2SX	12.2(17d)SXB2以降に移行		
12.2SXA	12.2(17d)SXB1以降に移行		

12.2SXB	12.2(17d)SXB1		
12.2SXD			12.2(18)SXD
12.2SY	12.2(17d)SXB2以降に移行		
12.2SZ	12.2(20)S4に移行		
12.2T	12.2(13)T14		
	12.2(15)T12		
12.2YT	12.2(15)T13以降に移行		
12.2YU	12.3(4)T6以降に移行		
12.2YV	12.3(4)T6以降に移行		
12.2YZ	12.2(20)S4以降に移行		
12.2ZC	12.3T以降に移行		
12.2ZD	12.3以降に移行		
12.2ZE	12.3以降に移行		
12.2ZF	12.3(4)T6以降に移行		
12.2ZG	12.3(4)T6以降に移行		

12.2ZH	12.3(4)T6以降に移行		
12.2ZI	12.2(18)S以降に移行		
12.2ZJ	12.3以降に移行		
12.2ZL	12.3(7)T以降に移行		
12.2ZN	12.3(2)T6以降に移行		
12.2ZO	12.2(15)T12以降に移行		
12.2ZP	12.3(8)XY以降に移行		
該当する 12.3 ベースのリリース	リビルド	Interim	メンテナンス
12.3	12.3(3f)		
	12.3(5c)		
	12.3(6a)		
			12.3(9)
12.3BC			12.3(9a)BC
12.3B	12.3(5a)B2		
12.3BW	12.3(5a)B2以降に移行		

12.3JA			12.3(2)JA
12.3T	12.3(2)T6		
	12.3(4)T6		
			12.3(7)T
12.3XA	12.3(7)T以降に移行		
12.3XB	12.3(8)T以降に移行		
12.3XC	12.3(2)XC3以降への移行が必要		
12.3XD	12.3(4)XD4		
12.3XE	12.3(2)XE1		
12.3XF	12.3(11)T以降に移行		
12.3XG	12.3(4)XG2		
12.3XH	12.3(11)T以降に移行		
12.3XI			12.3(7)XI
12.3XJ	12.3(7)XJ		
12.3XK	12.3(4)XK1		

12.3XL			12.3(7)XL
12.3XM			12.3(7)XM
12.3XN	12.3(14)T以降に移行		
12.3XQ	12.3(4)XQ		
12.3XR			12.3(7)XR
12.3XS	12.3(7)XS		
12.3XT	12.3(2)XT		
12.3XU	12.3(8)XU		
12.3XX			12.3(8)XX
12.3XW			12.3(8)XW
12.3XY			12.3(8)XY
12.3XZ			12.3(2)XZ
12.3YA			12.3(8)YA
12.3YD			12.3(8)YD
12.3YE			12.3(4)YE

12.3YF			12.3(11)YF
12.3YG			12.3(8)YG
12.3YH			12.3(8)YH

ソフトウェアのアップグレードを検討する場合は、http://www.cisco.com/en/US/products/products_security_advisories_listing.htmlおよび後続のアドバイザリも参照して、侵害を受ける可能性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。情報が不明な場合は、Cisco Technical Assistance Center(TAC)にお問い合わせください。

推奨事項

$propertyAndFields.get("recommendations")

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-20050126-ipv6

改訂履歴

リビジョン 1.0	2005年1月26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。