



Cisco Security Advisory: Crafted IPv6 Packet Causes Reload

Revision 1.0

最終更新日 2005 年 7 月 29 日 8:00 UTC

公開日 2005 年 7 月 29 日 8:00 UTC

目次

- 要約
- 該当製品
- 詳細
- 影響
- ソフトウェアバージョンおよび修正
- 修正ソフトウェアの入手
- 回避策
- 不正利用事例と公表
- この通知のステータス INTERIM
- 情報配信
- 更新履歴
- シスコセキュリティ手順

要約

Cisco Internetwork Operating System (IOS) Software 巧妙に細工された IPv6 パケットによる攻撃に対してサービス妨害 (Denial of Service (DoS))、および潜在的に任意のコードを実行できる脆弱性が存在します。本脆弱性を利用するにはパケットはローカル・ネットワークセグメントから送信されなくてはなりません。明示的に IPv6 トラフィックを処理するように設定された機器のみが影響を受けます。本脆弱性を悪用された場合には機器の再起動が発生する可能性やさらなる悪用にさらされる可能性があります。

シスコでは、本脆弱性対処用の無償のソフトウェアを提供しています。

本アドバイザリは以下にて確認可能です。

<http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>

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。

該当製品

脆弱性が存在する製品

影響を受けるのは、IPv6を利用可能なIOSでIPv6が設定されており、脆弱性が存在するバージョンの IOS を使用する全ての製品です。

IPv6をサポートしている機器であってもインタフェースを停止すれば本脆弱性に該当しません。各インタフェースにおいてIPv6を

完全に停止するには、no ipv6 address と no ipv6 enable の両方のコマンドを設定しなければなりません。IPv6を設定した場合と設定していない場合における show ipv6 interface コマンドの出力例を以下に示します。

システムで IPv6 が設定されていない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。

```
Router#show ipv6 int  
-ここの表示が空白になります。
```

下記の表示の場合は脆弱性があります

```
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  
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 が設定されているルータでは、ipv6 unicast-routing がグローバルに設定されていなくても、この問題に対する脆弱性が存在します。show ipv6 interface コマンドを使用すれば、いずれかのインターフェイスで IPv6 が設定されているかどうかを判別できます。

Cisco 製品で稼働中のソフトウェアを確認するには、機器にログインし show version コマンドを実行し、システムバナーを画面に表示します。Cisco IOS ソフトウェアは "Internetwork Operating System Software" もしくは単に "IOS" と表示します。そのすぐ後ろにイメージ名が括弧の間に表示され(場合により改行されています)、続いて "Version" と IOS リリース名が表示されます。(IOS 以外の)他の Cisco の機器は "show version" コマンドがない場合や、異なる表示をする場合があります。

以下の例は Cisco 製品で IOS リリース 12.3(6)、イメージ名 C2600-JS-MZ が稼働していることを示しています

```
Cisco Internetwork Operating System Software IOS (tm)  
C2600 Software (C2600-JS-MZ), Version 12.3(6), RELEASE SOFTWARE (fc1)
```

Cisco IOS の命名に関するさらなる情報は以下の URL を参照してください。

<http://www.cisco.com/warp/public/620/1.html>

脆弱性が存在しない製品

Cisco IOS が稼働していない製品は、影響を受けません。いずれかのバージョンの Cisco IOS が稼働していても、IPv6 に設定されたインターフェイスがない場合には、脆弱性は存在しません。

その他の製品について、本脆弱性の影響を受けるものは現在確認されていません。

詳細

IPv6 とは「Internet Protocol Version 6」のことで、これは、現在のインターネット プロトコルである IP Version 4 (IPv4) を置き換える目的で Internet Engineering Task Force (IETF) によって設計されたプロトコルです。

IPv6 パケットの処理に、脆弱性が存在します。論理インターフェイス（つまり、6to4 トンネルなどのトンネル）と物理インターフェイスのどちらでも、ローカルセグメントから受信した不正改造パケットで、本脆弱性が利用される可能性があります。不正改造パケットは6to4 トンネルを超えることも、トンネルの向こう側の機器に攻撃を行うこともできません。

本脆弱性を悪用するには、不正に改造された IPv6 パケットをローカルネットワークから送信する必要があり、1ホップ以上先から実行することはできません。

この問題は、Cisco Bug ID CSCef68324（登録ユーザのみ）で文書化されています。

影響

本脆弱性が悪用された場合、機器の再起動や、任意のコードを実行される結果となる場合があります。繰り返し悪用された場合、結果的に Dos 攻撃が継続したり任意のコードを実行される可能性があります。

ソフトウェアバージョンおよび修正

以下の Cisco IOS ソフトウェアの表の各行は、対象となるリリーストレイン、プラットフォームおよび製品群を示します。あるリリーストレインが脆弱である場合、修正が組み込まれている最も早いリリース（最初に修正されたリリース）とそれが利用可能となる予定日が“Rebuild” and “Maintenance”の列に示されます。リリーストレインで示されたリリースより前のものを使用している機器は脆弱であることが知られています。使用するリリースは少なくとも示されたリリース以降へアップグレードすることが推奨されます。

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Release	Rebuild	Maintenance
12.0S	12.0(26)S6	
	12.0(27)S5	
	12.0(28)S3	
	12.0(30)S2	12.0(31)S
12.0SX	Vulnerable; contact TAC	
	Vulnerable; migrate to 12.0(31)S or later	
12.0SL	Vulnerable; migrate to 12.0(31)S or later	
12.0ST	Vulnerable; migrate to 12.0(31)S or later	
12.0SY	Vulnerable; migrate to 12.0(31)S or later	
Affected 12.1-Based Release	Rebuild	Maintenance
12.1XU	Vulnerable; migrate to 12.3(15) or later	
12.1XV	Vulnerable; migrate to 12.3(15) or later	
12.1YB	Vulnerable; migrate to 12.3(15) or later	
12.1YC	Vulnerable; migrate to 12.3(15) or later	
12.1YD	Vulnerable; migrate to 12.3(15) or later	
12.1YE	Vulnerable; migrate to 12.3(15) or later	
12.1YF	Vulnerable; migrate to 12.3(15) or later	
12.1YH	Vulnerable; migrate to 12.3(15) or later	
12.1YI	Vulnerable; migrate to 12.3(15) or later	
Affected 12.2-Based Release	Rebuild	Maintenance
12.2B	Vulnerable; migrate to fixed 12.3(14)T2 or later	

12. 2BC	Vulnerable; contact TAC	
12. 2BW	Vulnerable; migrate to 12. 3(15) or later	
12. 2BY	Vulnerable; migrate to fixed 12. 3(14) T2 or later	
12. 2BX	Vulnerable; migrate to 12. 3(7) X14 or later	
12. 2BZ	Vulnerable; migrate to 12. 3(7) X14 or later	
12. 2CX	Vulnerable; contact TAC	
12. 2CY	Vulnerable; contact TAC	
12. 2CZ	Vulnerable; contact TAC	
12. 2DD	Vulnerable; migrate to fixed 12. 3(14) T2 or later	
12. 2DX	Vulnerable; migrate to fixed 12. 3(14) T2 or later	
12. 2EU	12. 2(20) EU1	
12. 2EW	Vulnerable; migrate to 12. 2(25) EWA	
12. 2EWA	12. 2(25) EWA1	
12. 2EX	Vulnerable; migrate to 12. 2(25) SEA or later	
12. 2EY	12. 2(25) EY1	
12. 2EZ		12. 2(25) EZ
12. 2JA	Vulnerable; migrate to 12. 3(4) JA or later	
12. 2JK	Vulnerable; contact TAC	
12. 2MB	Vulnerable; contact TAC	
12. 2MC	Vulnerable; migrate to 12. 4(2) MR	
12. 2MX	Vulnerable; migrate to fixed 12. 3(14) T2 or later	
12. 2S	12. 2(14) S14	
	12. 2(18) S9	
	12. 2(20) S8	
	12. 2(25) S4	
12. 2SE	Vulnerable; migrate to 12. 2(25) SEB or later	
12. 2SEA	Vulnerable; migrate to 12. 2(25) SEB or later	
12. 2SEB		12. 2(25) SEB
12. 2SEC		12. 2(25) SEC
12. 2S0	Vulnerable; contact TAC	
12. 2SU	Vulnerable; migrate to fixed 12. 3(14) T2 or later	
12. 2SV		12. 2(26) SV
12. 2SW	Vulnerable; contact TAC	
12. 2SX	Vulnerable; migrate to 12. 2(17d) SXB8 or later	
12. 2SXA	Vulnerable; migrate to 12. 2(17d) SXB8 or later	
12. 2SXB	12. 2(17d) SXB8	
12. 2SXD	12. 2(18) SXD4	
12. 2SXE	12. 2(18) SXE1	
12. 2SY	Vulnerable; migrate to 12. 2(17d) SXB8 or later	
12. 2SZ	Vulnerable; migrate to 12. 2(20) S8 or later	

12. 2T	12. 2(13) T16	
	12. 2(15) T16	
12. 2XA	Vulnerable; migrate to 12. 3(15) or later	
12. 2XB	Vulnerable; migrate to 12. 3(15) or later	
12. 2XC	Vulnerable; migrate to fixed 12. 3(14) T2 or later	
12. 2XD	Vulnerable; migrate to 12. 3(15) or later	
12. 2XE	Vulnerable; migrate to 12. 3(15) or later	
12. 2XF	Vulnerable; contact TAC	
12. 2XG	Vulnerable; migrate to 12. 3(15) or later	
12. 2XH	Vulnerable; migrate to 12. 3(15) or later	
12. 2XI	Vulnerable; migrate to 12. 3(15) or later	
12. 2XJ	Vulnerable; migrate to 12. 3(15) or later	
12. 2XK	Vulnerable; migrate to 12. 3(15) or later	
12. 2XL	Vulnerable; migrate to 12. 3(15) or later	
12. 2XM	Vulnerable; migrate to 12. 3(15) or later	
12. 2XN	Vulnerable; migrate to 12. 3(15) or later	
12. 2XQ	Vulnerable; migrate to 12. 3(15) or later	
12. 2XR	Vulnerable; migrate to 12. 3(4) JA or later	
12. 2XT	Vulnerable; migrate to 12. 3(15) or later	
12. 2XU	Vulnerable; migrate to 12. 3(15) or later	
12. 2XW	Vulnerable; migrate to 12. 3(15) or later	
12. 2XZ	Vulnerable; migrate to 12. 3(15) or later	
12. 2YT	Vulnerable; migrate to 12. 2(15) T16 or later	
12. 2YU	Vulnerable; migrate to fixed 12. 3(14) T2 or later	
12. 2YV	Vulnerable; migrate to fixed 12. 3(14) T2 or later	
12. 2YZ	Vulnerable; migrate to 12. 2(20) S8 or later	
12. 2ZA	Vulnerable; migrate to 12. 2(17d) SXB8 or later	
12. 2ZC	Vulnerable; migrate to fixed 12. 3(14) T2 or later	
12. 2ZD	Vulnerable; contact TAC	
12. 2ZE	Vulnerable; migrate to 12. 3(15) or later	
12. 2ZF	Vulnerable; migrate to fixed 12. 3(14) T2 or later	
12. 2ZG	Vulnerable; contact TAC	
12. 2ZH	Vulnerable; migrate to fixed 12. 3(14) T2 or later	
12. 2ZJ	Vulnerable; migrate to fixed 12. 3(14) T2 or later	
12. 2ZL	Vulnerable; contact TAC	
12. 2ZN	Vulnerable; migrate to fixed 12. 3(14) T2 or later	
12. 2ZO	Vulnerable; migrate to 12. 2(15) T16 or later	
12. 2ZP	Vulnerable; contact TAC	
Affected 12. 3-Based Release	Rebuild	Maintenance
	12. 3(3h)	

12. 3	12. 3 (5e)	
	12. 3 (6e)	
	12. 3 (9d)	
	12. 3 (10d)	
	12. 3 (12b)	
	12. 3 (13a)	12. 3 (15)
12. 3B	12. 3 (5a) B5	
12. 3BC		12. 3 (13a) BC
12. 3BW	Vulnerable; migrate to fixed 12. 3 (14) T2 or later	
12. 3JA		12. 3 (4) JA
12. 3JK		12. 3 (2) JK
12. 3T	12. 3 (7) T9	
	12. 3 (8) T8	
	12. 3 (11) T5	
	12. 3 (14) T2	
12. 3XA	Vulnerable; contact TAC	
12. 3XB	Vulnerable; migrate to fixed 12. 3 (14) T2 or later	
12. 3XC	12. 3 (2) XC3	
12. 3XD	Vulnerable; contact TAC	
12. 3XE	Vulnerable; contact TAC	
12. 3XF	Vulnerable; migrate to fixed 12. 3 (14) T2 or later	
12. 3XG	Vulnerable; contact TAC	
12. 3XH	Vulnerable; migrate to fixed 12. 3 (14) T2 or later	
12. 3XI	12. 3 (7) XI4	
12. 3XJ	Vulnerable; migrate to 12. 3 (11) YF3 or later	
12. 3XK	Vulnerable; contact TAC	
12. 3XL	Vulnerable; contact TAC	
12. 3XM	Vulnerable; migrate to fixed 12. 3 (14) T2 or later	
12. 3XQ	12. 3 (4) XQ1	
12. 3XR	12. 3 (7) XR4	
12. 3XS	Vulnerable; migrate to 12. 4 (1) or later	
12. 3XT	Vulnerable; contact TAC	
12. 3XU	Vulnerable; migrate to 12. 4 (2) T or later	
12. 3XW	Vulnerable; migrate to 12. 3 (11) YF3 or later	
12. 3XX	Vulnerable; migrate to 12. 4 (1) or later	
12. 3XY	Vulnerable; migrate to fixed 12. 3 (14) T2 or later	
12. 3YA	12. 3 (8) YA1	
12. 3YD	Vulnerable; contact TAC	
12. 3YF	12. 3 (11) YF3	
12. 3YG	12. 3 (8) YG2	
12. 3YH	Vulnerable; migrate to 12. 3 (8) YI1 or later	
12. 3YI	12. 3 (8) YI1	

12. 3YJ	12. 3(11)YJ	
12. 3YK	Vulnerable; contact TAC	
12. 3YQ	12. 3(14)YQ1	
12. 3YS		12. 3(11)YS
12. 3YT		12. 3(14)YT
12. 3YU		12. 3(14)YU
Affected 12. 4-Based Release	Rebuild	Maintenance
12. 4		12. 4(1)
12. 4MR		12. 4(2)MR
12. 4T		12. 4(2)T

“Rebuild” および “Maintenance” の用語に関する情報は以下をご参照ください。

<http://www.cisco.com/warp/public/620/1.html>

ソフトウェアのアップグレードを検討する際には、

http://www.cisco.com/en/US/products/products_security_advisories_listing.html およびそれ以降のアドバイザリも参照して、状況と完全なアップグレード ソリューションを判断してください。

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。情報が不明確な場合は、Cisco Technical Assistance Center (TAC) にお問い合わせください。

修正ソフトウェアの入手

ご契約を有するお客様

ご契約を有するお客様は、通常の経路でそれを 入手してください。ほとんどのお客様は、シスコのワールドワイドウェブサイト上の ソフトウェアセンターから入手することができます。 <http://www.cisco.com>

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡して、ソフトウェア アップグレードに関する支援を受けてください。この支援は通常無料です。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、シスコの Technical Assistance Center (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 (北米以外からの有料通話)
- 電子メール : tac@cisco.com

無料アップグレードの対象であることをご証明いただくために、製品のシリアル番号を用意し、このお知らせの URL を知らせてください。 サポート契約をご利用でないお客様に対する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。

ソフトウェアのアップグレードに関し、“psirt@cisco.com” もしくは “security-alert@cisco.com” にお問い合わせいただくことはご遠慮ください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、その他の TAC の連絡先情報については、<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> を参照してください。

お客様がインストールしたり、サポートを受けたりできるのは、ご購入いただいたフィーチャーセットに対してのみです。そのようなソフトウェア アップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用すると、お客様は <http://www.cisco.com/public/sw-license-agreement.html> にあるシスコのソフトウェア ライセンスの条項または <http://www.cisco.com/public/sw-center/sw-usingswc.shtml> にある Cisco.com のダウンロードに示されるその他の条項に従うことに同意したことになります。

回避策

回避策の効果は、お客様の状況、使用製品、ネットワークポロジ、トラフィック の性質や組織の目的に依存します。影響製品が多種多様であるため、回避策を実際に 展開する前に、対象とするネットワークで適用する回避策が最適であるか、お客様のサービスプロバイダーやサポート組織にご相談ください。

IPv6 が不要なネットワークにおいては、IOS 機器の IPv6 処理を停止することで本脆弱性にさらされることを回避できます。

不正利用事例と公表

本脆弱性は 2005 年 7 月 27 日 Black Hat security conference で公開されました。

この通知のステータス: **INTERIM**

本アドバイザリー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を示唆するものでもありません。本アドバイザリー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。またシスコシステムズは本ドキュメントの変更や更新を実施する権利を有します。シスコは、6週間以内にこの通知をアップデートする予定です。

後述する情報配信の URL を省略し、本アドバイザリーの記述内容に関して、独自の複製・ 意識を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

本アドバイザリーは、以下のシスコのワールドワイドウェブサイト上に掲載されます。

<http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>

ワールドワイドのウェブ以外にも、次の電子メールおよび Usenet ニュースの受信者向けに、この通知のテキスト版がシスコ PSIRT PGP キーによるクリア署名つきで投稿されています。

- cust-security-announce@cisco.com
- first-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

この通知に関する今後の最新情報は、いかなるものもシスコのワールドワイドウェブに掲載される予定です。しかしながら、前述のメーリングリストもしくはニュースグループに 対し積極的に配信されるとは限りません。この問題に関心があるお客様は上記 URL にて最 新情報をご確認いただくことをお勧めいたします。

更新履歴

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関する支援、およびシスコからセキュリティ情報を入力するための登録方法について詳しく知るには、シスコワールドワイドウェブサイトの http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。このページにはシスコのセキュリティ通知に関してメディアが問い合わせる際の指示が掲載されています。全てのシスコセキュリティアドバイザリは <http://www.cisco.com/go/psirt> で確認することができます。