IPv6 巧妙に細工された パケットの脆弱性

severity	**アドバイザリーID :** cisco-sa-20050729-ipv6 **初公開日 :** 2005-07-29 08:00 **バージョン 2.0 :** Final **回避策 :** Yes **Cisco バグ ID :** CSCuk53918 , CSCef68324	CVE-2005-2451

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インターネットワーク オペレーティング システム（IOS®）ソフトウェアはとりわけ巧妙に細工された IPv6 パケットからのサービス拒否 （DoS）および可能性としては任意 の コード実行攻撃に脆弱です。 パケットはローカルネットワーク セグメントから送信 する必要があります。 IPv6 トラフィックを処理するために明示的に設定されたデバイスだけ影響を受けています。 不正利用の成功に、デバイスはそれ以上の不正利用に開くリロードするか、またはかもしれません。

シスコはこの脆弱性に対処するソフトウェア アップデートをリリースしました。

このアドバイザリは 729-ipv6 で掲示されます。

該当製品

修正済みソフトウェア

この問題はサポートする影響を与え、のために、IPv6 設定されます Cisco IOS または Cisco IOS XR コードの取りはずされたバージョンを実行するすべての Ciscoデバイスに。 システムは IPv6 をサポートする、IPv6 のために明確に設定されなくて、影響を受けていません。 IPv6 がシステムで有効に なるかどうか判別する**提示 IPv6 interface コマンドを**使用できます。

提示 IPv6 interface コマンドの出力例は 2 つのシステム、1 IPv6 のために設定されないおよび IPv6 のために設定される 1 のために下記に示されています。

IPv6 がシステムで無効またはサポートされていない場合空出力か エラーメッセージは表示する。

```
Router#show ipv6 int fa 0/0

-here you see blank output
```

下記の例でシステムは脆弱です。

```
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#
```

IPv6 があるルータは物理的のか論理インターフェイスで IPv6 ユニキャストルーティングがグローバルに無効でもですこの問題に脆弱 有効に なりました。 **提示 IPv6 interface コマンドが** IPv6 があらゆるインターフェイスで有効に なるかどうか判別するのに使用することができます。

注: システムがイメージを自動的に基づかせていた 7600 シリーズ 12.2(17a)SX、12.2(17b)SXA または 12.2(17d)SXB を実行するおよび Cisco 6500 Multi Protocol Label Switching（MPLS）が有効に なる インターフェイスの IPv6 を有効に します。 MPLS は **MPLS IP** または **Tagスイッチング IP** コマンドによってインターフェイスで有効に なります。 IPv6 があらゆるインターフェイスで有効に なるかどうか判別する **提示 IPv6** interface コマンドを使用できます。

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」と表示されます。 出力次の行で、イメージ名は「バージョンに」先行しているかっこと IOSリリース名の間で表示する。 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 C2600-JS-MZ のイメージ名と IOS リリース 12.3(6) を実行する製品を示したものです:

```
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#
```

Cisco IOS リリース指名についてのその他の情報は http://www.cisco.com/web/about/security/intelligence/ios-ref.html で見つけることができます。

システムはまたもし設定するなら IPv6 のためのこの脆弱性から 3.2 以前の Cisco IOS XR バージョンを実行している影響を受けます。 **提示 IPv6 interface コマンドが** IPv6 が Cisco IOS XR を稼動するシステムで有効に なるかどうか識別するのに使用することができます。

脆弱性を含んでいないことが確認された製品

Cisco IOS か Cisco IOS XR を実行していない製品は影響を受けていません。

Cisco IOS のバージョンを実行する持っていない製品は IPv6 設定済みインターフェイス 脆弱ではないです。

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。

改訂履歴

Revision 1.8	2005-August-11	中間から最終に変更されるステータス。
Revision 1.7	2005-August-05	Cisco IOS XR のためにアップデートされるソフトウェア バージョン および 修正 表。
Revision 1.6	2005-August-03	Affected Products セクションにメモを付け加えました。 12.2EZ のためにアップデートされるソフトウェア バージョン および 修正 表。
Revision 1.5	2005-August-02	12.2JK、12.2MC、12.2ZD、12.3XA、12.3XE、12.3XG および 12.3XK のためにアップデートされるソフトウェア バージョン および 修正 表; 取除かれた 12.2CZ。
リビジョン 1.4	2005-August-01	12.2BC、12.2EZ、12.2SEB および 12.2SW のためにアップデートされるソフトウェア バージョン および 修正 表。
リビジョン 1.3	2005-July-31	アップデートされるソフトウェア バージョン および 修正 表。
リビジョン 1.2	2005-July-30	該当製品に追加される IOS XR。 行う回避策 セクションの変更を言い表わします。 アップデートされるソフトウェア バージョン および 修正 表。

リビジョン 1.1	2005-July-29	アップデートされるソフトウェア バージョン および 修正 表。 アップデートされる脆弱性が存在する製品 セクションの最初段落。
リビジョン 1.0	2005-July-29	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。