Cisco IOSソフトウェア 巧妙に細工されたTCPパケット サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20100324-tcp
初公開日 : 2010-03-24 16:00
最終更新日 : 2012-09-21 19:12
バージョン 1.1 : Final
CVSSスコア : 7.1
回避策 : Yes
Cisco バグ ID : CSCsz75186

CVE-2010-0577

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 IOS ® ソフトウェアはリモート非認証攻撃者が影響を受けたデバイスがリロードするか、またはハングしますことを可能にするかもしれないサービス拒否の脆弱性から影響を受けます。 TCP セッション確立フェーズの間に受け取られる脆弱性は巧妙に細工された TCP オプションが含まれている TCP セグメントによって引き起こされるかもしれません。 仕様に加えて、巧妙に細工された TCP オプションは、デバイスこの脆弱性が影響を受ける特別なコンフィギュレーションがなければなりません。

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 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-tcp で掲示されます。

注: 2010 年 3月 24 日、Cisco IOSソフトウェア Security Advisory によって組み込まれる書は 7 つのセキュリティ アドバイザリが含まれています。 すべてのアドバイザリは Cisco IOSソフトウェアの脆弱性に対処します。 各アドバイザリには、そのアドバイザリで詳述された脆弱性を解決するリリースを記載しています。 次の URLリストの表は正しい 2010 年 3月 24 日送達されたすべての Cisco IOSソフトウェア脆弱性、またはそれ以前ことリリースします:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-bundle

"Cisco Event Response: 半年ごと Cisco IOSソフトウェア Security Advisory は次のリンクのパブリケーションを」組み込みました:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar10.html

該当製品

修正済みソフトウェア

脆弱 な デバイスは Cisco IOSソフトウェアの影響を受けたバージョンを実行して、次のいずれかのために設定されます:

- 特定の TCP ウィンドウ サイズ
- TCP パスMTU ディスカバリ（PMTUD）
- 転送 プロトコルとして TCP のステートフルなネットワークアドレス変換（SNAT）

特定の TCP ウィンドウ サイズを使用するコンフィギュレーション

デバイスで起きる接続のために仕様 TCP レシーブ ウィンドウ サイズを使用するために設定されるデバイスはこの脆弱性から影響を受けます。 仕様 TCP レシーブ ウィンドウ サイズで設定されるデバイスに設定で次のコマンドがあります:

```
ip tcp window-size <window size, from 0 to 1073741823>
```

TCP ウィンドウ サイズがコマンド **ip tcp window-size <window サイズ**で明示的に設定されない場合、**0 から 1073741823> へ**のそれからデバイスは脆弱性から影響を受けません。

パスMTU ディスカバリを使用するコンフィギュレーション

デバイスで起きるか、または終端させる TCP 接続のために PMTUD を使用するために設定されるデバイスはまたこの脆弱性から影響を受けます。 異なる Cisco IOS ソフトウェアの機能は機能ごと の 基礎の PMTUD を有効に するか、またはディセーブルにすることを割り当てるかもしれません。 次のリストは TCP 接続のための PMTUD を有効に するために知られている機能があります:

- IPv4 上の TCP: **ip tcp path-mtu-discovery コマンドは**デバイスからの IPv4 接続上のすべての新しい TCP のための PMTUD を有効に します。 このコマンドはデフォルトでは無効になっています。
- IPv6 上の TCP: PMTUD は IPV6 のためにデフォルトで有効に なり、無効である場合もありません。
- ボーダー ゲートウェイ プロトコル（BGP）: Cisco IOSソフトウェアの最近のバージョンは（Cisco IOS Release 12.2(33)SRA は、12.2(31)SB、12.2(33)SXH、12.4(20)T およびそれ以降リリースします）自動的に BGP が設定されるときすべての BGP 隣接 セッションのための PMTUD を有効に します。 詳細については http://www.cisco.com/en/US/docs/ios/12_2sr/12_2sra/feature/guide/srbgpmtu.html を参照して下さい。

トンネル伝送する総称ルーティング カプセル化（GRE）のようなその他の機能、IP-in-IP および Layer 2 Tunneling Protocol （L2TP）はまた PMTUD の使用を可能にします。 ただし従って、これらは TCP サービスと関連していないし、この脆弱性から影響を受けません。

転送 プロトコルとして TCP のステートフル NAT を使用するコンフィギュレーション

SNAT を使用するために設定されるデバイスはまたこの脆弱性から影響を受けます。 転送 プロトコルとして TCP と SNAT を使用するために設定されるデバイスに設定で次のコマンドがあります:

```
ip nat Stateful id <stateful NAT ID number>
     redundancy <redundancy group name>
          ...
          protocol   tcp
!
```

SNAT コンフィギュレーションシナリオの下で影響を受けるために、SNAT 転送 プロトコルが TCP である必要があることに注目して下さい。 Cisco IOSソフトウェアの最近のバージョンは SNAT 転送 プロトコル（UDP をサポートします）として SNAT の使用がデバイスを脆弱にしなければだけ、TCP の使用をサポートしません。 SNAT はデフォルトで有効に ならないし、SNAT が設定されるとき Cisco IOS ソフトウェア リリースが SNAT のための転送 プロトコルとして TCP をサポートする場合、デフォルト の 転送 プロトコルは TCP です。

Cisco IOS ソフトウェア バージョンの判別

Cisco 製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、機器にログインし show version コマンドを実行してシステムバナーを表示させます。 "Internetwork Operating System Software"、"Cisco IOS Software" あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。 イメージ名は「バージョン」および Cisco IOS ソフトウェアリリース名によって、続かれて括弧内に表示する。 他の Cisco 機器では、 show version コマンドがない場合や、表示が異なる場合があります。

以下の例は、Cisco 製品にて、IOSリリース 12.3(26) が稼動し、そのイメージ名が C2500-IS-L であることを示しています:

```
Router#show version
Cisco Internetwork Operating System Software IOS (tm) 2500 Software (C2500-IS-L), Version
12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

<output truncated>
```

次の例は C1841-ADVENTERPRISEK9-M のインストール済みイメージ名前と Cisco IOS ソフトウェア リリース 12.4(20)T を実行している Cisco製品を指定したものです:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE
```

```
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

Cisco IOS ソフトウエアのリリース命名規則の追加情報は以下のリンクの "White Paper: Cisco IOS Reference Guide" で確認できます: http://www.cisco.com/warp/public/620/1.html。

脆弱性を含んでいないことが確認された製品

Cisco IOS XR ソフトウェアは影響を受けていません。

Cisco IOS XE ソフトウェアは影響を受けていません。

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。

改訂履歴

リビジョン 1.0	2010-March-24	初版リリース

利用規約