複数の IOSベース シスコ製品の TCP 脆弱性

severity	**アドバイザリーID :** cisco-sa-20040420-tcp-ios	CVE-2004-0230
	初公開日 : 2004-04-20 21:00	
	バージョン 2.1 : Final	
	回避策 : Yes	
	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

トランスミッション コントロール プロトコル（TCP） 仕様（RFC793）の脆弱性は外部研究者によって検出されました。 不正利用の成功は以前に公に説明されていたより大いに短い時間の確立された TCP 接続をリセットすることを敵が可能にします。 アプリケーションによっては、接続は自動的に再確立されて得るかもしれません。 それ以外の場合、ユーザは操作を繰り返さなければなりません（たとえば、新しい Telnet か SSH セッションを開いて下さい）。 攻撃されたプロトコルによっては、不正侵入の成功は考慮する必要がある終えられた接続を越える追加結果があるかもしれません。 この攻撃 ベクトルはセッションにだけ適当ですデバイスで（ルータ、スイッチ、またはコンピュータのような）およびないデバイスをだけ通っているセッションに終了している（たとえば、ルータによってルーティングされている）トランジットトラフィック。 さらに、この攻撃 ベクトルは直接データ統合か機密保持を妥協しません。

TCP スタックが含まれているすべてのシスコ製品はこの脆弱性に敏感です。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040420-tcp-ios で利用でき、Cisco IOSÂ® ソフトウェアを実行するシスコ製品に適用すると同時にこの脆弱性を記述します。

Cisco IOSソフトウェアを実行しない製品のためのこの脆弱性を記述する関連アドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040420-tcp-nonios で利用できます。

該当製品

修正済みソフトウェア

TCP スタックが含まれている製品はこの脆弱性に敏感です。 すべてのシスコ製品およびモデ

ルは影響を受けています。 公開の重大度は TCP を利用するアプリケーションおよびプロトコルに左右されます。

この攻撃 ベクトルはセッション デバイスで (ルータ、スイッチ、またはコンピュータのような) 終了しているとないデバイスをだけ通っているセッションにだけ適当です (たとえば、ルータによってルーティングされている) トランジットトラフィック。

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。

改訂履歴

Revision 2.1	2005-April-13	詳細 セクションの固定壊れたリンク。
Revision 2.0	2004-July-14	12.0SL のための修正を用いる更新済固定 Cisco IOS ソフトウェア リリースおよびマイグレーション パス 表。
Revision 1.9	2004-June-16	セクション 12.0S の復帰改行文字が付いている更新済固定 Cisco IOS ソフトウェア リリースおよびマイグレーション パス表
Revision 1.8	2004-May-20	最終に変更されるステータス。
Revision 1.7	2004-May-10	12.0(28)、12.0(27)S、12.2(23)、12.2(22)S、12.3(6)、および 12.2JA の Cisco IOS Firewall テーブル メンテナンス修正のための固定 Cisco IOSソフトウェア イメージをアップデートしました。
Revision 1.6	2004-May-04	12.0W5 のためのソフトウェア バージョン および 修正 セクション、更新済エントリおよび 12.2SX。 BGP MD5 シークレットの情報の更新済回避策 セクション。
Revision 1.5	2004-Apr-30	12.1 のためのソフトウェア バージョン および 修正 セクション、更新済エントリでは、12.3T FW、および 12.1DA。 12.3T IOS の追加された新しいセクション主要な、12.2 ベースのリリース。
リビジョン 1.4	2004-Apr-28	詳細 セクション DoD ドラフト TCP プロトコルへの追加されたリンク。 開発 および 公示 セクションでは、最初の文の変更された言葉遣い。
リビジョン	2004-Apr-25	ソフトウェア バージョン および 修正 セクションでは、アドバイザリの追加された序段落。

1.3		エントリ 12.1AY のためのソフトウェア バージョン および 修正 セクションでは、更新済 Cisco IOS ソフトウェア リリースおよびマイグレーション パス 表、12.2BX、12.2XB、12.2T および 12.2SXB。 更新済回避策 セクションではネットワークエッジ エントリの設定 アンチスプーフィング手段のためのコマンド シーケンス。
リビジョン 1.2	2004-Apr-22	ソフトウェア バージョン および 修正 セクションでは、12.1E エントリのための更新済 Cisco IOS Firewall 表。 エントリ 12.2SXA のためのソフトウェア バージョン および 修正 セクション、更新済 Cisco IOS ソフトウェア リリースおよびマイグレーション パス 表では、12.2SXB、12.1EW、12.2S、12.3T、12.2JA、12.1EA。
リビジョン 1.1	2004-Apr-21	ソフトウェア バージョン および 修正 セクション、Cisco IOS ソフトウェア リリースおよびマイグレーション パス 表では、更新済 12.1(20)E2 エントリ。 ソフトウェア バージョン および 修正 セクション、Cisco IOS ソフトウェア リリースおよびマイグレーション パス 表では、12.1E セクション、更新済 12.1(13)E13 エントリ。 ソフトウェア バージョン および 修正 セクション、Cisco IOS ソフトウェア リリースおよびマイグレーション パス 表では、12.1E セクション、更新済 12.1(13)E14 エントリ。 ソフトウェア バージョン および 修正 セクション、Cisco IOS ソフトウェア リリースおよびマイグレーション パス 表では、12.2T セクション、更新済 12.2(13)T12 エントリ。 ソフトウェア バージョン および 修正 セクション、Cisco IOS ソフトウェア リリースおよびマイグレーション パス 表では、12.2T セクション、更新済 12.2(13)T11 エントリ。 Workaround セクションでは、この行アップデートされる部分を制限するパケットレート: access-list 103 割り当て TCP ホスト 10.1.1.1
リビジョン 1.0	2004-Apr-20	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。