複数のシスコ製品の TCP 状態操作サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20090908-tcp24

初公開日 : 2009-09-08 00:00

バージョン 1.1 : Final

CVSSスコア : 7.8

回避策 : Yes

Cisco バグ ID : CSCsv04836

CVE-2008-4609

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

複数のシスコ製品はトランスミッション コントロール プロトコル（TCP）接続の状態を処理するサービス拒否（DoS）脆弱性から影響を受けます。 TCP 接続の状態の処理によって、攻撃者は長命状態を、可能性のある不明確に維持するために TCP 接続を強制する可能性があります。 十分な TCP 接続が長命か不明確な状態に強制である場合、攻撃の下のシステムのリソースは新しい TCP 接続が受け入れられることを防ぎます消費されるかもしれ。 場合によっては、システム 再度ブートするは標準 システム オペレーションを回復 して必要かもしれません。 これらの脆弱性を不正利用するために、攻撃者は脆弱 な システムの TCP 3 ウェイ ハンドシェイクを完了できる必要があります。

これらの脆弱性に加えて、Cisco Nexus 5000 デバイスはシステム クラッシュという結果に終るかもしれない TCP DoS 脆弱性が含まれています。 この追加脆弱性は TCP 状態操作脆弱性のテストの結果として発見されました。

Cisco は Cisco Webサイトからこれらの脆弱性に対処するダウンロードのためのフリーソフト アップデートをリリースしました。 これらの脆弱性に対しては回避策があります。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090908-tcp24 で掲示されます。

該当製品

修正済みソフトウェア

以下のシスコ製品にこれらの脆弱性から影響を受ける TCP 実装があります。 修正済みソフト

ウェアの情報に関してはソフトウェア バージョン および 修正 セクションを参照して下さい。

Cisco IOS ソフトウェア

Cisco製品で動作している Cisco IOS® ソフトウェア リリースを判別するために、管理者はデバイスにログイン し、システムバナーを表示する **show version コマンドを**発行できます。 "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。 その後ろにイメージ名が括弧の間に表示され、続いて "Version" と Cisco IOS ソフトウエア リリース名が表示されます。 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/web/about/security/intelligence/ios-ref.html

Cisco IOS XE ソフトウェア

Cisco製品で動作している Cisco IOS XE ソフトウェアのバージョンは Command Line Interface （ CLI ）からの **show version コマンド**を使用して判別することができます。

Cisco CatOS ソフトウェア

Cisco製品で動作している Cisco CatOS ソフトウェアのバージョンは CLI からの **show version コマンド**を使用して判別することができます。

Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア（ASA）および Cisco PIX

バージョン 7.1、7.2、8.0、および 8.1 を実行する Cisco ASA および Cisco PIX セキュリティ アプライアンス モデルは次の機能の何れかのために設定されたとき影響を受けています:

- SSL VPN
- ASDM 管理アクセス
- Telnet 経由のアクセス
- SSH アクセス
- リモートアクセス VPN のための Cisco トンネリング 制御プロトコル（cTCP）
- 仮想 Telnet
- バーチャルHTTP
- 暗号化された音声 インスペクション用の Transport Layer Security （TLS）プロキシ
- ネットワーク アクセスのカットスルー プロキシ

Cisco ASA および Cisco PIX セキュリティ アプライアンス モデルで動作しているソフトウェアのバージョンは CLI からの **show version コマンド**を使用して判別することができます。

Cisco NX-OS ソフトウェア

Nexus 5000 および 7000 シリーズ デバイスを on Cisco 実行している Cisco NX-OS ソフトウェアのバージョンは CLI からの **show version コマンド**を使用して判別することができます。

Scientific Atlanta 製品

Scientific Atlanta 顧客はこの文書で説明されている脆弱性の影響、軽減および治療に関する質問に関しては Scientific Atlanta のテクニカル サポートに連絡することを学びます。

Scientific Atlanta テクニカル サポートのための連絡先 情報は次の Webサイトで見つけることができます:

http://www.cisco.com/en/US/products/ps10459/serv_group_home.html

Linksys 製品

Cisco は Linksys 製品 グループを調査し、Linksys 製品が TCP 脆弱性から影響を受けないことが分りました。 Linksys 製品の追加質問の顧客は連絡する必要があります:

security@linksys.com

脆弱性を含んでいないことが確認された製品

以下のシスコ製品は影響を受けていません:

- Cisco IOS XR
- モジュール型 Cisco IOS ソフトウェア
- Cisco ASA ソフトウェア バージョン 8.2
- Cisco ASA および Cisco PIXソフトウェアバージョン 7.0
- Cisco PIXソフトウェアバージョン 6.x およびそれ以前
- Cisco Firewall Services Module（FWSM）
- Cisco マルチレイヤ ディストリビューションスイッチ（MD）
- Ciscoアプリケーション コントロール エンジン（ACE）モジュールおよびアプライアンス
- Cisco ACE XML Gateway
- Cisco Access Control Server（ACS）ソリューション エンジン
- Cisco ガード
- Ciscoセキュリティ モニタリング、分析および応答システム（CS-MARS）
- Cisco ONS 15000
- Cisco Content Services は切り替えます（CSS）
- Cisco Wide Area Application Services（WAAS）
- Cisco Wireless LAN Controller（WLC）
- IronPort C、M、S および X シリーズ アプライアンス
- Cisco グローバルサイトセレクタ（GSS）
- Cisco SSL サービス モジュール（SSLM）
- Cisco Network Analysis Module（NAM; ネットワーク解析モジュール）
- Cisco Content Switch Module（CSM）
- Cisco Webアプリケーション ファイアウォール（WAF）
- Cisco Service Control エンジン（SCE）
- Ciscoワイヤレス サービス モジュール（WiSM）
- Cisco Application and Content Networking System（ACNS）
- Cisco Content Engine（CE）

Cisco PSIRT は FINWAIT1 状態の TCP 接続が一時的に TCP 接続システム リソースをクリア オペレーティング システム結局消費するかもしれないが Linux および Microsoft Windows オペレーティング システムに基づいているテストし、それを見つけましたシスコ製品を。 十分なシステム リソースが消費される場合、支えられた DoS 状態は可能性のあるであるかもしれません。 この結果はシステムの設定および使用方法で依存性が高いです。 詳細についてはこれらの脆弱性が Microsoft Windows オペレーティング システムにどのようにに関する影響を及ぼすか、次のリンクで次のマイクロソフト社Webサイトを参照して下さい:

http://go.microsoft.com/fwlink/?LinkId=155978

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	2009-	脆弱性が存在しない製品リストに

ヨン 1.3	September-28	追加される; 更新済ソフトウェア テーブル。
リビジョン 1.2	2009-September-16	Linksys 製品および不正利用事例と公式発表 セクションのための Affected Products セクションを修正しました
リビジョン 1.1	2009-September-11	更新済脆弱 な ソフトウェア
リビジョン 1.0	2009-September-08	初版リリース

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。