Cisco Firewall サービス モジュール HTTPS 要求サービス拒否の脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20070214-CVE-2007-0964 **初公開日 :** 2007-02-14 20:38 **バージョン 1.0 :** Final **CVSSスコア :** 2.7 **回避策 :** Yes **Cisco バグ ID :**	CVE-2007-0964

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

3.1(3.18) 以前の Cisco Firewall サービス モジュール バージョンは非認証を可能にする可能性がある一時サービス拒否（DoS）状態を作成するために脆弱性がリモート攻撃者含まれています。

脆弱性はネットワーク アクセスを認める前にユーザを認証するために設定されるデバイスで不正な HTTPS を処理するとき エラーが原因要求しますです。 非認証は HTTPS プロトコルを利用する外部のウェブサイトにアクセスするように試みによって、リモート攻撃者この脆弱性を不正利用する可能性があります。 この操作は一時 DoS 状態に終って、リロードするために Cisco Firewall サービス モジュールを強制する可能性があります。

Cisco は Security Advisory のこの脆弱性を確認し、更新済ソフトウェアをリリースしました。

不正侵入の成功は攻撃者により Cisco Firewall サービス モジュールはリロードしますことを可能にします。 デバイスは自動的に再起動しま、一時 DoS 状態を引き起こします。 繰り返された不正侵入が拡張状態を作成するのに利用できます。 脆弱性がただ HTTPS 要求自体およびない URL の処理のエラーが原因で発生するので、攻撃者は多分悪意のあるトラフィックを生成するカスタム アプリケーションを利用しなければなりません。 攻撃者はエクスプロイトを行うのに標準 Webブラウザを活用できてまずないです。

該当製品

修正済みソフトウェア

3.1(3.18) 以前の Cisco Firewall サービス モジュール バージョンは脆弱です。

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

バージョン	説明	Section	ステータス	日付
1.0	初版リリース	該当なし	Final	2007 年 2 月 14 日

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。