Cisco CSS Content Services Switch および脆弱性をスプーフィングする ACE アプリケーション制御エンジン HTTP SSL ヘッダ

Medium	**アドバイザリーID :** Cisco-SA-20100702-CVE-2010-1575 **初公開日 :** 2010-07-02 14:15 **最終更新日 :** 2012-07-14 14:00 **バージョン 3.0 :** Final **CVSSスコア :** 3.5 **回避策 :** No Workarounds available **Cisco バグ ID :**	CVE-2010-1575

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 CSS Content Services Switch （CSS）、SSL サービス モジュール（SSLM）、および ACE アプリケーションは制御エンジン（ACE）認証される可能にする可能性がある HTTP 要求にスプーフィングされた SSL ヘッダを挿入するために脆弱性がリモート攻撃者含まれています。

SSL セッション 終了を行う場合の該当製品が弱く HTTP 証明書ヘッダの権限を実施するので存在 する脆弱性。 認証されて SSL 終了のための該当製品に通じる要求にスプーフィングされた SSL 証明書ヘッダを挿入することによって、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。 成功すれば、攻撃者は機密情報へのアクセス権を得る man-in-the-middle攻撃を行えますかもしれません。

Cisco はソフトウェア リリース メモ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。

この脆弱性は CSS または SSLM インストールに影響を与える可能性があります CSS の次のコンフィギュレーションステートメントによってクライアント 認証 検証を行うために設定されたインストールのより大きい影響を持つ可能性があります: **ssl サーバ <** SSLM の**コンテキスト >http-header クライアント証明書**および次の ssl **プロキシ ポリシー HTTP ヘッダ** コンフィギュレーションステートメント: **クライアント証明書。**

最終的に、この脆弱性の影響は影響を受けた CSS デバイスの背後にあるアプリケーションによってそれらのデバイスが HTTP 要求全体の複数の SSL ヘッダの存在をどのように処理するか決まり。 アプリケーションが要求に現われる最後のヘッダを処理すれば、CSS によって追加されたそれらを受け取ります SSL ヘッダの他のどの処理も間違ったヘッダの処理という結果に終る可能性があります。

該当製品

CSS 動作は Cisco バグ ID CSCsz04690 で文書化されています

Cisco はこの問題を報告するためにバーチャル セキュリティ研究に、LLC、ジョージ D. Gal 研究者感謝します。

脆弱性のある製品

この脆弱性は Cisco CSS デバイス、SSLM および ACE モジュールに影響を与えます。 SSL ヘッダ挿入は ACE モジュールのためのバージョン A2(3.0) に最初に現われました; ACE アプライアンスはヘッダ挿入を行わないし、影響を受けていません。

CSS 実行するデバイス バージョン 8.10.6.03 S またはそれ以降、か 8.20.4.03 S またはそれ以降は最初にに CSS の自身のヘッダを追加 する前に削除します要求の HTTP ヘッダを設定することができます。 これらのバージョンのデフォルト 設定はこれらのヘッダを削除することではないですがもし設定するなら **ssl 前取除 http hdr** と影響を受けていません。

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。

回避策

CSS で、ssl **サーバ < コンテキスト >http-header は**サーバ管理者の新しいクライアント 認証に付加されるランダム ヘッダ プレフィックスを定義することを許可によって**プレフィックス < RANDOM_PREFIX >** コマンド更にスプーフィング露出からのヘッダを保護します。

CSS のためのこのコマンドの使用方法および設定は CSS コマンドレファレンスで文書化されています。

SSLM で、次の ssl **プロキシ ポリシー HTTP ヘッダ** コンフィギュレーションステートメントは SSLM 挿入されたヘッダに付加される設定されたプレフィックスを挿入します: **prefix < プレフィックス >。 また SSLM で、ヘッダー名は次の ssl プロキシ ポリシー HTTP ヘッダ コンフィギュレーションステートメントによって変更されるかもしれません: エイリアス < エイリアス ストリング > < ヘッダー名 >。**

SSLM のためのこのコマンドの使用および設定は SSL サービス モジュール コマンドレファレンスで文書化されています。

さらに、CSS と 8.20.4.03 S および 8.10.6.03S を、次の新しいコマンド設定されましたリリースします: **ssl 前取除 http hdr**。 このコマンドは新しいヘッダを挿入する前に既存のヘッダを削除します。 たとえば、ソフトウェアがクライアント 認証情報のために設定されれば、このコマンドは既存のクライアント 認証ヘッダを削除しました、それから新しいヘッダは挿入されます。 この機能がプレフィックスと作動しないことに注目して下さい。 デフォルトの動作は挿入の前にヘッダを無視し続けます。 **ssl 前取除 http hdr** コマンドはデフォルトの動作に戻りません。 このコマンドは現在のヘッダの数に基づいて CSS パフォーマンスに影響を与えるかもしれません。

SSL ヘッダ挿入はバージョン A2(3.0) の ACE モジュールで最初に設定されました。 SSL ヘッダ挿入機能は ACE アプライアンスにありません。

ACE モジュールはソフトウェア バージョン A2(3.0) のための ACE コンフィギュレーション ガイドで文書化されているようにヘッダ削除および書き直しを可能にします。

修正済みソフトウェア

Cisco カスタマは 1-800-553-2447 か 1-408-526-7209 でまたは tac@cisco.com で E メールで Cisco Technical Assistance Center にコンタクトをとってアップグレードを入手できます。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20100702-CVE-2010-1575

改訂履歴

Version	Description	Section	Status	日付
1.0	初版リリース	該当なし	Final	2010-Jul-02

利用規約

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。