Cisco Webセキュリティアプライアンスの HTTPSパケット処理におけるDoS脆弱性

High

アドバイザリーID : cisco-sa-20160302-wsa

初公開日 : 2016-03-02 16:00

バージョン 1.0 : Final

CVSSスコア : 7.8

回避策 : No workarounds available

Cisco バグ ID : CSCuu24840

CVE-2016-1288

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 Webセキュリティアプライアンス(WSA)のWebプロキシフレームワークの脆弱性により、認証されていないリモートの攻撃者が、信頼できるネットワーク内からセキュアな接続をネゴシエートする機能を使用して、該当デバイスにサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、HTTPSパケットの不適切な処理に起因します。攻撃者は、該当デバイスを介して不正なHTTPS要求パケットを送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はDoS状態を作成し、WSAを通過するすべての要求がドロップされる可能性があります。この状態は一時的なものであり、機能を復元するために手動による介入は必要ありません。

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ています。この脆弱性を軽減する回避策はありません。

このアドバイザリは次のリンクで確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-wsa

該当製品

脆弱性のある製品

この脆弱性は、8.5.3-051および9.0.0-485より前のAsyncOSを実行しているCisco Webセキュ

リティアプライアンス(WSA)に影響を与えます。

WSAで実行されているソフトウェアバージョンを確認するには、 **version**コマンドを使用します。次の例は、ソフトウェアバージョン7.5.1-079を実行しているシステムでの、このコマンドの出力を示しています。
CiscoCowsa>バージョン
現在のバージョン
==========
製品：Cisco IronPort S670 Webセキュリティアプライアンス
モデル：S670
バージョン：7.5.1-079

デバイスがこの脆弱性の影響を受けるには、HTTPSプロキシ機能を有効にする必要があります。

WSAでHTTPSプロキシ機能が有効になっているかどうかを確認するには、次の手順に従います。

1. WSAのWeb管理インターフェイスにログインします。
2. [Security Services] > [HTTPS Proxy] に移動します。
3. 機能のステータスを確認します。HTTPSプロキシ機能は、[Enable HTTPS Proxy] 設定にチェックマークが付いている場合に有効になります。

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。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- Cisco Eメールセキュリティアプライアンス(ESA)（仮想バージョンとハードウェアバージョンの両方）
- Ciscoセキュリティメールアプライアンス(SMA)（仮想バージョンとハードウェアバージョンの両方）

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は

http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載のシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する場合は、 http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成は新規リリースでも継続して適切なサポートが受けられることを確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。
http://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

この脆弱性は、Cisco Webセキュリティアプライアンス(WSA)ソフトウェアバージョン8.5.3-051以降および9.0.0-485以降で修正されています。

ほとんどの場合、WSAは、 **System Administration** GUIの **System Upgrade**オプションを使用して、ネットワーク経由で更新できます。 **System Administration** GUIを使用してデバイスをアップグレードするには、次の手順を実行します。

1. **System Administration > System Upgrade**の順に選択します。
2. [Upgrade Options] をクリックします。
3. [Download] オプションを選択します。
4.アップグレードに必要なリリースを選択します。
5. 「アップグレード**準備」領域で**、適切なオプションを選択します。
6. [Proceed] をクリックしてアップグレードを開始します。アップグレードのステータスを示す経過表示バーが表示されます。

アップグレードが完了すると、デバイスがリブートします。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-wsa

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	-	Final	2016 年 3 月 2 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。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。