Cisco適応型セキュリティアプライアンスのCLIにおけるリモートコード実行の脆弱性

Medium	**アドバイザリーID :** cisco-sa-20160817-asa-cli **初公開日 :** 2016-08-17 18:45 **最終更新日 :** 2016-08-18 21:12 **バージョン 1.1 :** Final **CVSSスコア :** 6.8 **回避策 :** No workarounds available **Cisco バグ ID :** CSCtu74257	CVE-2016-6367

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適応型セキュリティアプライアンス(ASA)ソフトウェアのコマンドラインインターフェイス(CLI)パーサーの脆弱性により、認証されたローカルの攻撃者がサービス妨害(DoS)状態を作成したり、任意のコードを実行したりする可能性があります。攻撃者は、該当デバイスで特定の無効なコマンドを呼び出すことで、この脆弱性を不正利用する可能性があります。

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。この脆弱性に対処する回避策はありません。このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-cli

該当製品

脆弱性のある製品

8.4(3)よりも前のCisco適応型セキュリティアプライアンス(ASA)ソフトウェアリリースには脆弱性が存在します。攻撃者がこの脆弱性を不正利用するには、ローカルアクセス権を持ち、認証される必要があります。

次の製品で実行されている該当Cisco ASAソフトウェアは、この脆弱性の影響を受ける可能性があります。

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco ASA 5500-X シリーズ次世代ファイアウォール

- Cisco PIX Firewall*
- Cisco Firewall Services Module(FWSM)*

修正済みリリースの詳細については、「修正済みソフトウェア」セクションを参照してください。

***注**：Cisco Firewall Service Module(FWSM)およびCisco PIX Firewallは、公開されているEnd of Life(EoL)文書に記載されているソフトウェアサポートのマイルストーンの最終日を過ぎています。これらのデバイスに対するさらなる調査は行われず、修正済みソフトウェアは提供されません。詳細については、次のEoLドキュメントを参照してください。

- Cisco Firewall Services Module（FWSM）
  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/catalyst-6500-series-firewall-services-module/eol_c51-699134.html
- Cisco PIX ファイアウォール
  http://www.cisco.com/c/en/us/products/security/pix-500-series-security-appliances/eos-eol-notice-listing.html

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

この脆弱性に対処する回避策はありません。

この脆弱性をトリガーするには、攻撃者が認証される必要があります。お客様のインフラストラクチャにおける役割を考慮すると、ネットワークデバイスは脅威の攻撃対象として貴重なターゲットであり、そのように保護する必要があります。シスコでは、すべてのネットワーキングベンダーのお客様に対して、セキュリティ侵害を防止および検出するための運用手順を含めることを推奨しています。Cisco ASAデバイスを保護し、ネットワーク全体のセキュリティを強化するために役立つ情報が記載されている『 Cisco ASAファイアウォールの強化に関するシスコガイド』を参照してください。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する際には、[シスコのセキュリティアドバイザリおよびアラート（Cisco Security Advisories and Alerts）] ページで入手できるシスコ製品のアドバイザリを定期的に参照して、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が新規リリースで引き続き正しくサポートされていることを十分に確認してください。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。

修正済みリリース

次の表に、この脆弱性に対する修正を含む最初のソフトウェアリリースを示します。

Cisco ASA メジャー リリース	First Fixed Release (修正された最初のリリース)
7.2	影響あり。8.4(3) 以降への移行が必要
8.0	影響あり。8.4(3) 以降への移行が必要
8.1	影響あり。8.4(3) 以降への移行が必要
8.2	影響あり。8.4(3) 以降への移行が必要
8.3	影響あり。8.4(3) 以降への移行が必要
8.4	8.4(3)
8.5	影響あり。9.0(1) 以降への移行が必要
8.6	影響あり。9.0(1) 以降への移行が必要
8.7	影響あり。9.0(1) 以降への移行が必要
9.0	9.0(1)
9.1	Not affected
9.2	Not affected
9.3	Not affected
9.4	Not affected
9.5	Not affected
9.6	Not affected

不正利用事例と公式発表

2016年8月15日、シスコはShadow Brokersグループによってオンラインに投稿された情報に対して警告を受けました。このグループは、Equation Groupからの開示を受けていると主張しています。公開された資料には、複数のベンダーのファイアウォール製品の不正利用が含まれています。記載されているシスコ製品は、PIXおよびASAファイアウォールです。

出典

この脆弱性の不正利用は、Shadow Brokersグループによって公開されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-cli

改訂履歴

バージョン	説明	セクション	ステータス	日付

1.1	最初の修正済みソフトウェアバージョンを明確にし、影響を受けるソフトウェアの表を追加。	該当製品、修正済みソフトウェア	Final	2016年8月18日
1.0	初回公開リリース	-	Final	2016年8月17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。