Cisco Web セキュリティ アプライアンスのレイヤ 4 トラフィック モニタにおけるセキュリティ バイパスの脆弱性

アドバイザリーID : cisco-sa-20180606-wsa CVE-2018-0353
初公開日 : 2018-06-06 16:00
最終更新日 : 2018-06-08 14:26
バージョン 1.1 : Final
CVSSスコア : 7.5
回避策 : No workarounds available
Cisco バグ ID : CSCvg78875

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) のトラフィック モニタリング機能の脆弱性により、認証されていないリモートの攻撃者が、レイヤ 4 トラフィック モニタ (L4TM) 機能を回避し、セキュリティ保護をバイパスできる可能性があります。

この脆弱性は、影響を受けるトラフィックのモニタリングを実行するオペレーティング システム ソフトウェアの変更に起因します。攻撃者は、巧妙に細工された IP パケットを該当デバイスに送信することによって、この脆弱性を不正利用できる可能性があります。攻撃者がこの不正利用に成功すると、WSA で拒否するように設定されていても、デバイスを通じてトラフィックを渡せるようになります。この脆弱性は、IPv4 と IPv6 の両方のトラフィックに影響します。

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-20180606-wsa

該当製品

脆弱性のある製品

この脆弱性は、WSA ソフトウェア用 Cisco AsyncOS (仮想およびハードウェア アプライアン

スの両方）で、バージョン 10.5.1、10.5.2、または 11.0.0 のいずれかの WSA ソフトウェアを実行している場合に影響を与えます。影響を受けるソフトウェア リリースの詳細については、本セキュリティ アドバイザリの「修正済みソフトウェア」セクションを参照してください。

WSA は、L4TM を設定している場合に脆弱です。WSA に L4TM が設定されているかどうかについては、管理者が L4 トラフィック モニタ設定にアクセスすることで確認できます。

1. [セキュリティサービス（Security Service）] > [L4トラフィックモニタ（L4 Traffic Monitor）] をクリックします
2. [グローバル設定の編集（Edit Global Settings）] をクリックします
3. [L4トラフィックモニタを有効化する（Enable L4 Traffic Monitor）] にチェックを入れ、必要なポートを選択します

WSA ソフトウェア バージョンの確認

脆弱性のある Cisco AsyncOS ソフトウェア バージョンが Cisco WSA で実行されているかどうかについては、管理者が WSA CLI の version コマンドを使用することで確認できます。以下に、Cisco AsyncOS ソフトウェア バージョン 10.5.1-296 を実行しているアプライアンスでの出力例を以下に示します。

```
<#root>

ciscowsa>

version
```

```
<#root>

Current Version
===============
Product: Cisco IronPort S670 Web Security Appliance
Model: S670
Version:

10.5.1-296


.
.
.
```

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

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。

- E メール セキュリティ アプライアンス（ESA）の仮想バージョンとハードウェア バージョンの両方
- Security Mail Appliance（SMA）の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 https://www.cisco.com/c/en/us/products/end-user-license-agreement.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。

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 TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

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。

修正済みリリース

次の表では、左の列に、WSA ソフトウェア用 Cisco AsyncOS のメジャー リリースを示しています。右の列は、メジャー リリースが本アドバイザリに記載している脆弱性に該当するかどうか、また、本脆弱性に対する修正を含む最初のマイナー リリースに該当するかどうかを示します。

次の表に示すように、適切なリリースにアップグレードする必要があります。

Cisco AsyncOS WSA ソフトウェア メジャー リリース	この脆弱性に対する最初の修正リリース
10.5.1 よりも前	脆弱性なし
10.5.1	10.5.2-042
10.5.2	10.5.2-042
11.0.0	11.5.0-0614

WSA の更新は、ほとんどの場合、システム管理 GUI の [システムアップグレード（System Upgrade）] オプションを使用することにより、ネットワーク経由で実行できます。システム管理 GUI を使用してデバイスをアップグレードする場合は、次の手順を実行します。

1. [システム管理（System Administration）] > [システムアップグレード（System Upgrade）] を選択します。
2. [アップグレードオプション（Upgrade Options）] をクリックします。
3. [ダウンロードしてインストール（Download and Install）] を選択します。
4. アップグレードするリリースを選択します。
5. [アップグレード準備（Upgrade Preparation）] 領域で、適切なオプションを選択します。
6. [続行（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。

出典

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-wsa

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	リリース 10.5.2-042 が入手できることを反映し、修正済みリリースの情報を更新。	修正済みソフトウェア	Final	2018 年 6 月 8 日
1.0	初回公開リリース	—	Final	2018 年 6 月 6 日

利用規約

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。