Cisco Eメールセキュリティアプライアンスの Eメールスキャナにおける DoS脆弱性

High

アドバイザリーID : cisco-sa-20151104-esa2

初公開日 : 2015-11-04 16:00

最終更新日 : 2015-11-20 17:48

バージョン 1.2 : Final

CVSSスコア : 7.8

回避策 : No workarounds available

Cisco バグ ID : CSCuv47151

CVE-2015-6291

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 Eメールセキュリティアプライアンス(ESA)向けCisco AsyncOSのEメールメッセージフィル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ESAデバイスをサービス妨害(DoS)状態のために使用不能にする可能性があります。

この脆弱性は、電子メールの添付ファイルに破損したフィールドが含まれており、ESAによってフィルタリングされている場合の不適切な入力検証に起因します。攻撃者は、ESAに添付ファイルを含む巧妙に細工された電子メールを送信することで、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状態を引き起こす可能性があります。添付ファイルのフィルタ処理中は、フィルタリングプロセスが再開されるまで、メモリが高速で消費されます。プロセスが再起動すると、同じ不正な添付ファイルの処理が再開され、DoS状態が継続します。
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、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151104-esa2

該当製品

脆弱性のある製品

この脆弱性は、仮想アプライアンスとハードウェアアプライアンスの両方のCisco AsyncOS for ESAに影響を与えます。

次のいずれかのルールを使用して設定されたメッセージフィルタによって、この脆弱性が発生する可能性があります。

- ボディーを含む
- attachment-contains
- every-attachment-contains
- attachment-binary-contains
- dictionary-match
- attachment-dictionary-match

デバイスにどのESAメッセージフィルタが設定されているかを確認するには、ESA CLIで **filters detail all**コマンドを使用します。次の例は、汎用メッセージフィルタを使用するように設定されているデバイスの結果を示しています。

esa.prompt> **filters detail all**

有効な有効な名前の数

1 Y Y example_filter

example_filter:if body-contains("example", 1) {

quarantine ("ポリシー") ;

} 脆弱性のある Cisco AsyncOS ソフトウェア バージョンが Cisco ESA で実行されているかどうかの確認は、管理者が ESA CLI の version コマンドを使用することで実施できます。Cisco AsyncOS ソフトウェア バージョン 8.5.3-051 を実行しているデバイスでの出力例を以下に示します。

```
ciscoesa> version
Current Version
===============
Product: Cisco IronPort X1070 Messaging Gateway(tm) Appliance
Model: X1070
Version: 8.5.3-051
.
.
.
```

CiscoクラウドEメールセキュリティ(CES)には、サービスソリューションの一部としてCisco ESAとCisco Security Management Appliance(SMA)が含まれています。シスコは、このソリューションに含まれる製品について、定期的なメンテナンスを行っています。お客様から Cisco CES サポートに連絡して、ソフトウェアのアップグレードを要求することもできます。

脆弱性を含んでいないことが確認された製品

次の製品は、この脆弱性の影響を受けません。

- Cisco Webセキュリティアプライアンス (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（仮想バージョンとハードウェアバージョンの両方）

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。

セキュリティ侵害の痕跡

この脆弱性のセキュリティ侵害のインジケータは、トラフィックがESAに影響を与えるかどうかです。トラフィックが影響を受けるかどうかを判断するには、ESA CLIで **workqueue status**コマンドを使用します。次の例は、トラフィックが影響を受けるESAの結果を示しています。

esa> **workqueue status**
ワークキューの状態を取得できませんでした：キューがマウントされていません

キューがマウントされていない場合、デバイスがこの脆弱性の影響を受けている可能性があります。ESAがこの脆弱性の影響を受ける場合は、Cisco Technical Assistance Center(TAC)にお問い合わせください。

回避策

この脆弱性を軽減する回避策はありません。

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場合は、 http://www.cisco.com/go/psirtにあるCisco Security Advisoriesアーカイブを参照し、後続のアドバイザリを確認して、侵害の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。

次の表では、左の列にCisco AsyncOS for ESAソフトウェアのメジャーリリースを示します。中央の列が示すのは、本アドバイザリに記載された脆弱性によるメジャー リリースへの影響の有無、また、本脆弱性に対する修正を含む最初のマイナー リリースです。右の列は、メジャーリリースが次のアドバイザリに記載されているすべての脆弱性の影響を受けるかどうかと、これらの脆弱性の修正を含むリリースを示しています。

- cisco-sa-20151104-aos
- cisco-sa-20151104-wsa
- cisco-sa-20151104-wsa1
- cisco-sa-20151104-wsa2
- cisco-sa-20150612-esa

- cisco-sa-20151104-esa2

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。

AsyncOS for ESA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	この脆弱性に対する最初の修正リリ
7.7以前	該当。8.5.7-043に移行してください。	該当。8.5.7-043以降に移行してくだ
8.0または8.0.1	該当。8.5.7-043に移行してください。	該当。8.5.7-043以降に移行してくだ
8.0.2	該当。9.1.1-023に移行してください。	該当。9.1.1-023以降に移行してくだ
8.5	8.5.7-043	8.5.7-043 以降
9.0	該当。9.1.1-023に移行してください。	該当。9.1.1-023以降に移行してくだ
9.1	9.1.1-023	9.1.1-023 以降
9.5	該当。9.6.0-046に移行してください。	該当。9.6.0-046以降に移行してくだ
9.6	9.6.0-046	9.6.0-046 以降
9.7	Not affected	Not affected

ほとんどの場合、ESAはネットワーク経由で更新できます。これには、**System Administration** GUIの**System Upgrade**オプションを使用します。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する（Download and Install）] オプションを選択するか、ESA の場合はアップグレードを [ダウンロード（Download）]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-20151104-esa2

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.2	GUIを使用してデバイスをアップグレードする手順を追加。	修正済みソフトウェア	Final	2015年11月20日
1.1	CESのメンテナンスとアップグレードに関する情報を追加。	脆弱性が存在する製品	Final	2015年11月16日
1.0	初回公開リリース	-	Final	2015 年 11 月 4 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。