

Cisco Eメールセキュリティアプライアンスフィルタバイパスの脆弱性

| | | |
|--------|--|-------------------------------|
| Medium | アドバイザリーID : cisco-sa-20170118-esa | CVE-2017-3800 |
| | 初公開日 : 2017-01-18 16:00 | |
| | 最終更新日 : 2017-01-19 14:45 | |
| | バージョン 1.1 : Final | |
| | CVSSスコア : 5.8 | |
| | 回避策 : No workarounds available | |
| | Cisco バグ ID : CSCuz16076 | |

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)用Cisco AsyncOSソフトウェアのコンテンツスキャンエンジンにおける脆弱性により、認証されていないリモートの攻撃者がデバイス上で設定されたメッセージまたはコンテンツフィルタをバイパスできる可能性があります。

この脆弱性は、さまざまな形式の電子メールメッセージ添付ファイルの入力検証が不完全であることに起因します。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メッセージを送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はESAで設定されているコンテンツまたはメッセージフィルタをバイパスできる可能性があります。このメッセージフィルタバイパスにより、マルウェアを含む電子メールの添付ファイルがターゲットデバイスを通過する可能性があります。

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-20170118-esa>

該当製品

脆弱性のある製品

この脆弱性は、着信Eメールの添付ファイルにメッセージフィルタまたはコンテンツフィルタ

を適用するようにソフトウェアが設定されている場合、Cisco Eメールセキュリティアプライアンス用Cisco AsyncOSソフトウェアの最初の修正済みリリースより前のすべてのリリース（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）に影響します。この脆弱性は、メッセージフィルタまたはコンテンツフィルタの特定のルールまたはアクションに限定されません。

該当するソフトウェアリリースの詳細については、このアドバイザリの冒頭に記載されているCisco Bug IDを参照してください

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製品には影響を与えないことを確認しました。

- Ciscoコンテンツセキュリティ管理アプライアンス、仮想バージョンとハードウェアバージョン
- 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

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

修正済みソフトウェア リリースの詳細については、本アドバイザリ上部のCisco Bug IDを参照ください。

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。

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

シスコは、この脆弱性を報告していただいたVerizonのセキュリティ研究者であるParvez Anwar氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170118-esa>

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 | セキュリティ研究者の会社名を追加。 | 出典 | Final | 2017年1月19日 |
| 1.0 | 初回公開リリース | - | Final | 2017年1月18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、単独の転載や意識を施した場合、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。