Cisco E メール セキュリティ アプライアンス 不正 な EML 添付ファイル バイパス の 脆弱性

Medium	**アドバイザリーID :** cisco-sa-20170906-esa **初公開日 :** 2017-09-06 16:00 **最終更新日 :** 2017-09-18 12:40 **バージョン 1.1 :** Final **CVSSスコア :** 5.8 **回避策 :** Yes **Cisco バグ ID :** CSCuz81533	CVE-2017-12218

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）のための Cisco AsyncOS ソフトウェアの Advanced Malware Protection （AMP）内の malware 検出 機能の脆弱性はリモート攻撃者非認証によりエンドユーザに渡されるべき malware が含まれている電子メールの添付ファイルを引き起こすようにする可能性があります。

脆弱性は AMP の失敗が原因 malware が含まれている可能性があるある特定の EML 添付ファイルをスキャンするです。 攻撃者は目標とされたデバイスを通して巧妙に細工された EML 添付ファイルが付いている電子メールの送信によってこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者が設定された ESA 電子メール メッセージおよびコンテンツフィルタリングをバイパスし、malware がエンドユーザに配信されるようにことを可能にする可能性があります。

この脆弱性に対処する回避策があります。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170906-esa

該当製品

修正済みソフトウェア

この脆弱性は Cisco ESA のための Cisco AsyncOS ソフトウェアに、バーチャルおよび ESA

の着信 電子メールの添付ファイルをスキャンするためにメッセージまたはコンテンツ フィルターで設定されるハードウェア アプライアンス両方影響を与えます。 該当するソフトウェアリリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

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 Web セキュリティ アプライアンス、バーチャルおよびハードウェアバージョン
- Cisco コンテンツ セキュリティ管理アプライアンス、バーチャルおよびハードウェアバージョン

改訂履歴

Version	Description	Section	Status	日付
1.1	回避策を追加しました。	要約および回避策	Final	2017-September-18
1.0	Initial public release.		Final	2017 年 9 月 6 日

利用規約