

Cisco E メール セキュリティ アプライアンス EXE ファイル スキャン バイパスの脆弱性

Medium	アドバイザーID : cisco-sa-20180815-esa-file-bypass	CVE-2018-0419
	初公開日 : 2018-08-15 16:00	
	最終更新日 : 2018-08-20 16:31	
	バージョン 1.1 : Final	
	CVSSスコア : 5.3	
	回避策 : No workarounds available	
	Cisco バグ ID : CSCvh03786	

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) のある特定の添付ファイル検出 メカニズムの脆弱性はリモート攻撃者非認証が影響を受けたシステムのフィルタリング 機能をバイパスするようにする可能性があります。

脆弱性は実行可能ファイル (EXE) ファイル内の内容の不適切な検出が原因です。 攻撃者は ESA によって認識されないし、ブロックされるカスタマイズされた EXE ファイ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なにも疑わないユーザに悪意のある実行可能ファイルが含まれている電子メール メッセージを送信 する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はありません。

このアドバイザーは、次のリンクより確認できます。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180815-esa-file-bypass>

該当製品

脆弱性のある製品

この脆弱性は Cisco E メール セキュリティ アプライアンス (ESA) に影響を与えます。 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、このアドバイザーの上で 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

[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。](#)

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、[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) では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

Cisco はこの脆弱性を報告するために InteliSecure EMEA のリーアム Romanis に感謝することを望みます。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180815-esa-file-bypass>

改訂履歴

Version	Description	Section	Status	日付
1.1	脆弱性を報告した外部研究者を信じました。	Source	Final	2018-August-20

1.0	初回公開リリース		Final	2018年8月15日
-----	----------	--	-------	------------

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。