

Cisco EメールセキュリティアプライアンスのURLフィルタリングバイパスの脆弱性



アドバイザーID : cisco-sa-esa-url-bypass-sGcfsDrp

[CVE-2021-1534](#)

初公開日 : 2021-10-06 16:00

バージョン 1.0 : Final

CVSSスコア : [5.8](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvx60178](#)

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ソフトウェアのアンチスパム保護メカニズム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該当デバイスのURLレピュテーション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、URLの不適切な処理に起因します。攻撃者は、特定の方法でURLを巧妙に細工することで、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、攻撃者は該当デバイスに設定されているURLレピュテーションフィルタをバイパスし、悪意のあるURLがデバイスを通過できるようになる可能性があります。

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。

このアドバイザーは、次のリンクより確認できます。

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

該当製品

脆弱性のある製品

公開時点では、この脆弱性はリリース14.0.1より前のCisco ESA用Cisco AsyncOSソフトウェアに影響を与えました。

最も完全で最新の情報については、このアドバイザーの上部にあるバグ ID の詳細セクション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

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

[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 セキュリティ アドバイザリ 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アップグレードソリューション一式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。

修正済みリリース

発行時点では、次の表に記載されているリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左の列はシスコソフトウェアリリースを示し、右の列はリリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースを示しています。

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	First Fixed Release (修正された最初のリリース)
14.0 より前	修正済みリリースに移行。
14.0	14.0.1

修正済みリリースは、Cisco.comのSoftware Centerからは入手できません。管理者は、GUIまたはCLIを使用してソフトウェアをアップグレードできます。

ほとんどの場合、ソフトウェアは、Cisco ESAのWebインターフェイスのシステムアップグレードオプションを使用して、ネットワーク経由でアップグレードできます。Webインターフェイスを使用してデバイスをアップグレードするには、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. 適切な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。経過表示バーにアップグレードのステータスが表示されます。アップグレードが完了すると、デバイスが再起動します。

Product Security Incident Response Team (PSIRT; プロダクト セキュリティ インシデント レスポンス チーム) は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、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は確認しておりません。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

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

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2021-OCT-06

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。