Cisco Secure Web Applianceのリアルタイムスキャンアーカイブファイルバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-wsa-archive-bypass-Scx2e8zF　CVE-2026-20056
初公開日 : 2026-02-04 16:00
バージョン 1.0 : Final
CVSSスコア : 4.0
回避策 : No workarounds available
Cisco バグ ID : CSCwq69761

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 Secure Web Appliance用のCisco AsyncOSソフトウェアにおけるDynamic Vectoring and Streaming(DVS)エンジンの実装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アンチマルウェアスキャナをバイパスし、悪意のあるアーカイブファイルのダウンロードを可能にする可能性があります。

この脆弱性は、特定のアーカイブファイルの不適切な処理に起因します。攻撃者は、該当デバイスを介して巧妙に細工されたアーカイブファイ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。このアーカイブファイルはブロックされるはずです。エクスプロイトに成功すると、攻撃者はマルウェア対策スキャナをバイパスし、マルウェアをエンドユーザワークステーションにダウンロードできる可能性があります。ダウンロードされたマルウェアは、エンドユーザが悪意のあるファイルを抽出して起動しない限り、自動的には実行されません。

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-wsa-archive-bypass-Scx2e8zF

該当製品

脆弱性のある製品

公開時点では、この脆弱性はデバイス設定に関係なく、仮想バージョンとハードウェアバージ

ョンの両方でCisco Secure Web Applianceに影響を与えました。

このアドバイザリの公開時点で脆弱性が存在するシスコソフトウェアリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。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。

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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

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

シスコは、修正済みソフトウェアリリースへのアップグレードが利用可能になるまで、回避策や緩和策（適用可能な場合）を一時的な解決策と見なします。この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

修正済みリリース

発行時点では、次の表に示す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。

左側の列にはシスコソフトウェアリリース、右側の列に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が示されています。

Cisco Secure Web Appliance向けCisco AsyncOSリリース	First Fixed Release（修正された最初のリリース）
15.2 以前	15.2.5-011

ほとんどの場合、アプライアンスのWebインターフェイスで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ソフトウェアを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（Upgrade）] オプションをクリックします。
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. 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）] をクリックすると、アップグレードが始まります。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。

シスコの 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済み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

この脆弱性は Cisco Cisco Technical Assistance Center（TAC）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-wsa-archive-bypass-Scx2e8zF

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	2026年2月4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、単独の転載や意訳を施した場合、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。