

Cisco Secure Web Applianceの認証バイパスの脆弱性



アドバイザーID : cisco-sa-wsa-auth-bypass-6YZkTQhd

[CVE-2026-20152](#)

初公開日 : 2026-04-15 16:00

最終更新日 : 2026-04-16 13:14

バージョン 1.1 : Final

CVSSスコア : [5.3](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwr20696](#)

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(WSA)用のCisco AsyncOSソフトウェアの認証サービス機能の脆弱性により、認証されていないリモートの攻撃者が認証ポリシー要件をバイパスできる可能性があります。

この脆弱性は、HTTP要求でのユーザ指定の認証入力の検証が不適切なことに起因します。攻撃者は、特定の認証要求を含むHTTP要求を該当デバイスに送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はデバイスでのポリシーの適用をバイパスできる可能性があります。Cisco Secure Web Applianceには直接的な影響はありません。ただし、この脆弱性を不正利用した結果、攻撃者はデバイスを介して制限する必要があるHTTP要求を送信す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-wsa-auth-bypass-6YZkTQhd>

該当製品

脆弱性のある製品

この脆弱性は、公開時点でCisco Secure Web Applianceの仮想バージョンとハードウェアバー

ジョンの両方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。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- Cisco Secure Email Gateway、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
- 安全な電子メールと Web マネージャ、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

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

シスコでは、回避策や緩和策（該当する場合）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の一時的な解決策であると考えています。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用Cisco AsyncOSソフトウェアリリース	First Fixed Release (修正された最初のリリース)
15.2 より前	修正済みリリースに移行。
15.2	15.2.5-013

Cisco Secure Web Appliance用Cisco AsyncOSソフトウェアリリース	First Fixed Release (修正された最初のリリース)
15.5	修正済みリリースに移行。
16.0	影響なし。

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-auth-bypass-6YZkTQhd>

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	リリース15.5の情報を含む修正済みリリースを更新。	修正済みソフトウェア	Final	2026年4月16日
1.0	初回公開リリース	—	Final	2026年4月15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。