Cisco Secure Web Applianceレンジ要求バイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-swa-range-bypass-2BsEHYSu
初公開日 : 2025-02-05 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 : CSCwk58287

CVE-2025-20183

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ソフトウェアのポリシーベースのCisco Application Visibility and Control(AVC)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ウイルス対策スキャナを回避し、悪意のあるファイルをエンドポイントにダウンロードする可能性があります。

この脆弱性は、巧妙に細工された範囲要求ヘッダー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、巧妙に細工された範囲要求ヘッダーを含むHTTP要求を送信することにより、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、Cisco Secure Web Applianceで検出されることなく、ウイルス対策スキャナを回避してマルウェアをエンドポイントにダウンロードでき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-swa-range-bypass-2BsEHYSu

該当製品

脆弱性のある製品

公開時点で、この脆弱性はRange Request Forward機能が有効なCisco Secure Web Appliance（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。範囲要

求の転送はデフォルトで無効になっています。

範囲要求転送が有効になっているかどうかを確認します

Cisco Secure Web ApplianceでRange Request Forward機能が有効になっているかどうかを確認するには、CLIで管理者としてrangerequestdownloadコマンドを使用します。rangerequestdownload コマンドがRange requests are currently Enabledを返した場合は、次の例に示すように、Range Request Forward機能が有効になっています。

```
<#root>

cisco-wsa>

rangerequestdownload


Range requests are currently Enabled.

Are you sure you want to change the setting? [N]>
```

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。ただし、管理者はRange Request Forward機能を無効にすることで、この脆弱性を軽減できます。

範囲要求の転送はデフォルトで無効になっています。Range Request Forwardが有効な場合、管理者は次の例に示す手順を使用して無効にすることができます。

```
<#root>

cisco-wsa>

rangerequestdownload
```

```
Range requests are currently Enabled.
Are you sure you want to change the setting? [N]>
cisco-wsa>
```

Y

```
cisco-wsa>
```

commit

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。お客様は、最初に自社の環境への適用性と影響を評価する前に、回避策や緩和策を導入しないでください

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。

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 AsyncOS for Secure Web Appliance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）
14.0 以前	修正済みリリースに移行。
14.5	修正済みリリースに移行。
15.0	15.0.1-004
15.1	修正済みリリースに移行。
15.2	15.2.1-011

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。

アップグレードが完了すると、デバイスがリブートします。

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

この脆弱性は Cisco 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-swa-range-bypass-2BsEHYSu

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	2025年2月5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。