Cisco Cyber Vision Centerに保存されているクロスサイトスクリプティングの脆弱性

Medium

アドバイザリーID : cisco-sa-cv-xss-rwRAKAJ9
初公開日 : 2025-10-01 16:00
バージョン 1.0 : Final
CVSSスコア : 5.4
回避策 : No workarounds available
Cisco バグ ID : CSCwq56790 CSCwq56791

CVE-2025-20356
CVE-2025-20357

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 Cyber Vision CenterのWebベースの管理インターフェイスにおける複数の脆弱性により、認証されたリモートの攻撃者が、インターフェイスのユーザに対してクロスサイトスクリプティング(XSS)攻撃を実行する可能性があります。

これらの脆弱性は、該当システムのWebベースの管理インターフェイスでユーザ入力が十分に検証されないことに起因しています。攻撃者は、悪意のあるコードをインターフェイスの特定のページに挿入することで、これらの脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者は該当インターフェイスのコンテキストで任意のスクリプトコードを実行したり、ブラウザベースの機密情報にアクセスする可能性があります。

CVE-2025-20356を不正利用するには、攻撃者はSensor Explorerページへのアクセスを許可する有効な管理クレデンシャルを持っている必要があります。デフォルトでは、AdminおよびProductユーザロールにこのアクセス権があります。また、Sensorsページへのアクセスを許可するように設定されたすべてのカスタムユーザにも、このアクセス権が付与されます。

CVE-2025-20357を不正利用するには、攻撃者はレポートページへのアクセスを許可する有効な管理者クレデンシャルを持っている必要があります。デフォルトでは、定義済みのすべてのユーザロールがこのアクセス権を持ちます。レポートページへのアクセスを許可するように設定されているカスタムユーザも同様です。

シスコはこれら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。これら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-cv-xss-

rwRAKAJ9

該当製品

脆弱性のある製品

公開時点で、これらの脆弱性はデバイス設定に関係なく、Cisco Cyber Vision Centerに影響を与えていました。

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」セクションに記載されている製品のみが、これらの脆弱性の影響を受けることが分かっています。

シスコは、これらの脆弱性がCisco Cyber Vision Global CenterまたはCisco Cyber Vision Sensorには影響を与えないことを確認しました。

回避策

これら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、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、回避策や緩和策は一時的な解決策であると考えています。これらの脆弱性を完全に修正し、本アドバイザリで説明されている障害の発生を回避するために、お客様には本アドバイザリで説明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

公開時点では、次の表の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。

左の列にはシスコソフトウェアリリースが、右の列にはリリースがこのアドバイザリに記載された脆弱性の影響を受けるかどうか、およびこれら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。

CVE-2025-20356

シスコサイバービジョンセンター	First Fixed Release（修正された最初のリリース）
5.2 以前	修正済みリリースに移行。
5.3	脆弱性なし

CVE-2025-20357

シスコサイバービジョンセンター	First Fixed Release（修正された最初のリリース）
5.0 以前	脆弱性なし
5.1	修正済みリリースに移行。
5.2	修正済みリリースに移行。
5.3	脆弱性なし

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とその公表は確認しておりません。

出典

シスコは、これらの脆弱性を報告していただいたSchiphol社のJoost Spanjerberg氏およびSjoerd de Haas氏にVest Informatiebeiligingから感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cv-xss-rwRAKAJ9

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10月1日

利用規約

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。