

Cisco Identity Services Engineに保存されたクロスサイトスクリプティングの脆弱性



アドバイザリーID : cisco-sa-ise-xss-V2bm9JCY

初公開日 : 2024-08-07 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 : [CSCwj04195](#) [CSCwj04197](#)

[CVE-2024-20443](#)

[CVE-2024-20479](#)

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 Identity Services Engine(ISE)のWebベース管理インターフェイスにおける複数の脆弱性により、認証されたりモートの攻撃者が、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)攻撃を実行できる可能性があります。

これらの脆弱性の詳細については本アドバイザリーの「[詳細情報](#)」セクションを参照してください。

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-ise-xss-V2bm9JCY>

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 ISEに影響を与えました。

公開時点で脆弱性が確認されているCiscoソフトウェアのリリースについては、このアドバイザリーの「[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。

脆弱性を含ま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。

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために、他の脆弱性をエクスプロイトする必要はありません。また、いずれかの脆弱性の影響を受けるリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2024-20443: Cisco ISEストアドXSSの脆弱性

Cisco ISEのWebベース管理インターフェイスの脆弱性により、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XSS攻撃を実行する可能性があります。

この脆弱性は、該当システムのWebベース管理インターフェイスでユーザ入力の検証が不十分であることに起因します。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。この脆弱性を不正利用するには、攻撃者は該当デバイスに少なくとも低特権アカウントを持っている必要があります。

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。

バグID: [CSCwj04195](#)

CVE ID : CVE-2024-20443

セキュリティ影響評価 (SIR) : 中

CVSS ベーススコア : 5.4

CVSS ベクトル : CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

CVE-2024-20479: Cisco ISEストアドXSSの脆弱性

Cisco ISEのWebベース管理インターフェイスの脆弱性により、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XSS攻撃を実行する可能性があります。

この脆弱性は、該当システムのWebベース管理インターフェイスでユーザ入力の検証が不十分であることに起因します。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。この脆弱性を不正利用するには、攻撃者は該当デバイスの管理者権限を持っている必要があります。

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。

バグID:[CSCwj04197](#)

CVE ID : CVE-2024-20479

セキュリティ影響評価 (SIR) : 中

CVSS ベーススコア : 4.8

CVSS ベクトル : CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

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

[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。

左の列にはCiscoソフトウェアリリースが、右の列にはそのリリースが本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、またどのリリースにこれらの脆弱性に対する修正が含まれているかを示します。

Cisco ISE リリース	First Fixed Release (修正された最初のリリース)
2.7	修正済みリリースに移行。
3.0	修正済みリリースに移行。
3.1	3.1P9
3.2	3.2P7 (2024年9月)
3.3	3.3P3
3.4	脆弱性なし

デバイスのアップグレード手順については、[Cisco Identity Services Engine](#) サポートページにあるアップグレードガイドを参照してください。

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

これらの脆弱性を報告していただいたING Hubs Poland社のLaura Rowieska氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-V2bm9JCY>

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	2024年8月7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。