Cisco Identity Services Engineのストアド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-ise-xss-ubfHG75C **初公開日 :** 2023-02-15 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 6.1 **回避策 :** No workarounds available **Cisco バグ ID :** CSCwd19529	CVE-2023-20085

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の脆弱性により、認証されていないリモートの攻撃者が、該当デバイスのWebベース管理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。

この脆弱性は、該当デバイスのWebベース管理インターフェイスによる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、インターフェイスの特定のページに悪意のあるコードを挿入することで、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、攻撃者は影響を受けるインターフェイスのコンテキストで任意のスクリプトを実行したり、ブラウザベースの機密情報にアクセスしたり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-ise-xss-ubfHG75C

該当製品

脆弱性のある製品

この脆弱性は、Cisco ISEの脆弱性が存在するリリースを実行し、ポスチャ機能を有効にしているシスコデバイス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。

ポスチャが有効になっているかどうかの確認

ポスチャ機能が有効になっているかどうかを確認するには、次の手順に従います。

1. Cisco ISEのWebベース管理インターフェイスにログインします。
2. **Menu**アイコンをクリックします。
3. [Work Centers] を選択します。
4. [Posture] メニューを確認します。

Postureメニューが表示される場合、デバイスはこの脆弱性の影響を受けます。[Posture] メニューが表示されない場合、デバイスはこの脆弱性の影響を受けません。

注：ポスチャ機能は、Cisco ISEのプレミアライセンスに含まれています。詳細については、『Cisco ISEライセンスガイド』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、この脆弱性の影響を受けることが分かっています。

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

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 ISE リリース	First Fixed Release（修正された最初のリリース）
2.7 以前	脆弱性なし
3.1 以前	脆弱性なし
3.2	3.2 P1

デバイスのアップグレード手順については、Cisco Identity Service 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

この脆弱性は、シスコのRoberto Petrilloが社内セキュリティテストで発見しました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-ubfHG75C

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	2023年2月15日

利用規約

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。