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

Medium

アドバイザリーID : cisco-sa-ise-xss-42tgsdMG
初公開日 : 2025-02-05 16:00
バージョン 1.0 : Final
CVSSスコア : 4.8
回避策 : No workarounds available
Cisco バグ ID : CSCwj04202 CSCwk32089

CVE-2025-20205
CVE-2025-20204

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)攻撃を実行でき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ベース管理インターフェイスでユーザが行った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。これらの脆弱性を不正利用するには、攻撃者は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。

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-ise-xss-42tgsdMG

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。

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が存在する製品セクションにリストされている製品だけがこれら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、これらの脆弱性がCisco ISE Passive Identity Connector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

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。

左の列にはシスコソフトウェアリリースが、中央と右の列には、そのリリースがこのアドバイザリに記載された脆弱性のいずれかに該当するかどうか、また、その脆弱性に対する修正を含むリリースが記載されています。

Cisco ISE ソフトウェア リリース	CVE-2025-20204 の最初の修正済みリリース	CVE-2025-20205 の最初の修正済みリリース
3.0	修正済みリリースに移行。	修正済みリリースに移行。
3.1	修正済みリリースに移行。	修正済みリリースに移行。
3.2	3.2P8（2025年7月）	3.2P7
3.3	3.3P3	3.3P4
3.4	3.4P1	3.4P1

デバイスのアップグレード手順については、Cisco Identity Service Engineサポートページの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とその公表は確認しておりません。

出典

CVE-2025-20204：この脆弱性を報告していただいたポーランドのING HubsのLaura Rowieska氏に感謝いたします。また、この脆弱性を独自に報告していただいたDeloitte社のDan Marin氏、Teodor Cervinski氏、George Jubleanu氏、およびCristian Mocanu氏にも感謝いたします。

CVE-2025-20205：この脆弱性を報告していただいたポーランドのING Hubs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-42tgsdMG

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

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。