Cisco Identity Services Engineにおける複数の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-isexss-BS8ctE7U
初公開日 : 2026-04-15 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 : CSCwn85868 CSCwn87479

CVE-2026-20132

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、管理書き込み権限を持つ認証された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、ストアドクロスサイトスクリプティング(XSS)攻撃またはリフレクトXSS攻撃を実行する可能性があります。

これらの脆弱性は、Webページに保存されているユーザ指定のデータの不十分なサニタイズに起因します。攻撃者は、特定のリンクをクリックするか、該当するWebページを表示するようにインターフェイスのユーザを確信させることで、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。挿入されたスクリプトコードは、Webベースの管理インターフェイスのコンテキストで実行されるか、攻撃者が機密のブラウザベースの情報にアクセスできる可能性があります。

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-isexss-BS8ctE7U

該当製品

脆弱性のある製品

これらの脆弱性は、デバイスの設定に関係なく、Cisco ISEに影響します。

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。

脆弱性が Cisco ISE Passive Identity Connector（ISE-PIC）に影響しないことはシスコで確認済みです。

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、回避策や緩和策（該当する場合）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の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、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載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

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、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。

Cisco ISE リリース	First Fixed Release（修正された最初のリリース）
3.1 以前	修正済みリリースに移行。
3.2	3.2 パッチ 8
3.3	3.3 パッチ 5
3.4	3.4 パッチ 2
3.5	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。

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

これらの脆弱性は、Cisco Technical Assistance Center(TAC)の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-isexss-BS8ctE7U

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	2026年4月15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。