Cisco Identity Services Engineの強化リリース：2026年9月

Advisory ID : cisco-sa-hardening-ise-XU5EwX5T
初公開日 : 2026-09-16 16:00
バージョン 1.0 : Final
CVSSスコア : 10.0
回避策 : No workarounds available
Cisco Bug ID :

CVE-2026-20194
CVE-2026-20192
CVE-2026-20237
CVE-2026-20234
CVE-2026-20287
CVE-2026-20130

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

概要

予防的なセキュリティと製品の品質に対するシスコの継続的な取り組みの一環として、Cisco Identity Services Engine(ISE)およびCisco ISE Passive Identity Connector(ISE-PIC)のエンジニアリングチームは、包括的な内部セキュリティレビューを実施しました。このレビューの結果、社内で発見された複数の脆弱性に対処するソフトウェアのセキュリティ強化リリースが公開されました。

これらの脆弱性は、シスコの社内テストで発見されたものです。そのうちの1つが活発に不正利用されることが知られています。詳細については、「Cisco Identity Services Engine認証バイパスの脆弱性」を参照してください。 お客様によるパッチ適用を支援し、開示プロセスを効率化するために、シスコはこれらの問題をその根本的な脆弱性クラス（Common Weakness Enumeration（CWE））ごとに分類し、CWE の各グループに 1 つの共通脆弱性識別子（CVE ID）を割り当てました。

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-hardening-ise-XU5EwX5T

このアドバイザリは、アドバイザリグループの一部です。これらのアドバイザリとリンクの一覧については、2026年9月16日発行のCisco Advance Notification, Security Advisoriesを参照してください。

該当製品

脆弱性がある製品

これらの脆弱性は、デバイス設定に関係なく、Cisco ISEおよびISE-PICに影響を与えます。

脆弱性が存在する Cisco 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。

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の脆弱性の影響を受けることが知られています。

詳細

次の表に、この強化リリースで対処されている脆弱性クラスの概要を示します。各 CVE ID に割り当てられる CVSS スコアは、その特定の CWE カテゴリ内で最も影響の大きい 1 つの根本的な脆弱性がもたらす可能性がある最大のシビラティ（重大度）を表しています。

CVE ID	CVSS最高スコア	脆弱性クラス（最高レベルのCWE）	説明
CVE-2026-20130	10.0	CWE-74	ダウンストリームコンポーネントで使用される出力の特殊要素の不適切な無害化（コマンドインジェクション、クロスサイトスクリプティング、xmlインジェクション、コードインジェクション、およびリソースインジェクションを含む）
CVE-2026-20192	10.0	CWE-284	不適切なアクセスコントロール[1]（許可、認証、特権、バイパスを含む）
CVE-2026-20194	9.1	CWE-669	球体の間での不適切なリソース転送（転送時の機密情報の露出、保存前の機密情報の不適切な削除、および無制限のファイルアップロードを対象とする）
CVE-2026-20234	9.9	CWE-522	クレデンシャルの保護が不十分（情報漏えい、回復可能な形式でのパスワードの保存、およびパスワードの弱いエンコーディングが対象）

CVE ID	CVSS最高スコア	脆弱性クラス（最高レベルのCWE）	説明
CVE-2026-20237	9.9	CWE-20	不適切な入力検証（入力検証、パストラバーサル、外部パス制御など）
CVE-2026-20287	6.5	CWE-269	不適切な権限管理（不適切な権限割り当て、権限チェーン、および権限APIの不適切な使用を対象とする）

1. この脆弱性クラスに属する脆弱性の1つは、アクティブに不正利用されることが確認されています。詳細については、「Cisco Identity Services Engine認証バイパスの脆弱性」を参照してください。

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

これらの脆弱性を修正し、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。

修正リリース

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。右側の列は、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最初のリリースを示しています。このセクションで示すように、適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

Cisco ISE または ISE-PIC リリース	第 1 修正済みリリース
3.01 以前	修正済みリリースに移行します。
3.12	3.1パッチ12
3.22	3.2パッチ11
3.3	3.3パッチ12
3.4	3.4パッチ7
3.53	3.5パッチ4

1. Cisco ISEソフトウェアリリース3.0は ソフトウェアメンテナンスが終了しています。利用可能な強化修正を含むサポート対象リリースに移行することをお勧めします。
2. Cisco ISEソフトウェアリリース3.1および3.2は、 ソフトウェアメンテナンス段階にあります。これらのリリースには、重要なSIR脆弱性修正のみが含まれています。利用可能なすべての強化修正を含むサポート対象リリースに移行することをお勧めします。

3. Cisco ISE- PIC は販売終了日を迎えました。リリース 3.4 が、サポートされる最後のリリースです。

デバイスのアップグレード手順については、Cisco Identity Services Engine サポートページの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

すでに特記されている場合を除き、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、既存のテストプロセスおよびフロンティアの AI モデルを使用した内部セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ise-XU5EwX5T

改訂履歴

バージョン	説明	セクション	Status	日付
1.0	初版リリース	—	Final	2026年9月16日

利用規約

ソフトウェアのダウンロードおよびテクニカルサポート

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、マイデバイス（My Devices）ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定再販業者やシスコ認定パートナーを通じて調達されたもので、ライセンスが有効なものに限ります。

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。 無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバ

イザリの URL をご用意ください。

ソフトウェアのアップグレードを検討する際には、関連す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。

利用規約の詳細

シスコは、商品適格性または特定目的への適合性に関する保証を含め、明示的か黙示的かを問わず、いかなる種類の保証も表明しません。前述の一般論に限定されることなく、シスコは、本情報の正確性または完全性を保証するものではありません。コンテンツは「現状のまま」提供されます。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。

本セキュリティアドバイザリに含まれる情報のコピーや要約には、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。本セキュリティアドバイザリの最新版については、シスコ セキュリティ アドバイザリ ページをご覧ください。Cisco 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評価します。詳細については、シスコのセキュリティ脆弱性ポリシーを参照してください。

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。