

Cisco Identity Services Engine の脆弱性



Advisory ID : [cisco-sa-ise-multi-hrP9jQSQ](#) [CVE-2026-76424](#)
初公開日 : 2026-09-16 16:00 [CVE-2026-76423](#)
バージョン 1.0 : Final [CVE-2026-76428](#)
CVSSスコア : [10.0](#) [CVE-2026-76426](#)
回避策 : No workarounds available [CVE-2026-76425](#)
Cisco Bug ID : [CSCwu26055](#) [CSCwu26054](#) [CSCwu20156](#) [CSCwu27428](#) [CSCwu39998](#) [CSCwu43502](#)

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

Cisco Identity Services Engine(ISE)およびCisco ISE Passive Identity Connector(ISE-PIC)の複数の脆弱性により、リモート攻撃者が該当デバイスでREST APIへの認証をバイパスし、リモートコードを実行し、SQLインジェクションを実行し、XML外部エンティティインジェクション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-multi-hrP9jQSQ>

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。さらに、Cisco Identity Services Engineの改善と修正についてのその他のドキュメントについては、『[Cisco Identity Services Engineセキュリティ強化リリース：2026年9月](#)』を参照してください。

該当製品

脆弱性がある製品

CVE-2026-76423、CVE-2026-76426、およびCVE-2026-76428：これらの脆弱性は、デバイス設定に関係なく、Cisco ISEおよびCisco ISE-PICに影響を与えます。

CVE-2026-76424、CVE-2026-76425、およびCVE-2026-76427：これらの脆弱性は、デバイス設定に関係なく、Cisco ISEのみに影響します。

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別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェア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-2026-76423: Cisco ISE REST API認証バイパスの脆弱性

Cisco ISEおよびCisco ISE-PICのREST API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への管理アクセスを取得する可能性があります。

この脆弱性は、REST API Webサービスが十分な認可チェックで公開されないことに起因します。攻撃者は、エクスポートされたREST APIポートに巧妙に細工されたHTTP要求を送信することで、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、攻撃者は管理者権限でISEの設定とIDデータを読み取って変更でき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。

バグID: [CSCwu39998](#)

CVE ID : CVE-2026-76423

セキュリティ影響評価 (SIR) : 致命的

CVSS ベーススコア : 10.0

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

CVE-2026-76424: Cisco ISEの任意のファイルアクセスの脆弱性

Cisco ISEのREST APIの脆弱性により、認証されたりリモート攻撃者が該当デバイスに任意のファイルをアップロードまたはコピーできる可能性があります。

この脆弱性は、ファイル操作の不十分な検証に起因します。攻撃者は、巧妙に細工されたパスを含むファイルをアップロードすることにより、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、攻撃者は該当デバイスでルートとして任意の場所にファイルをアップロードし、任意のコマンドを実行できる可能性があります。この脆弱性をエクスプロイトするには、攻撃者は有効な管理者ログイン情報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: [CSCwu26055](#)

CVE ID : CVE-2026-76424

セキュリティ影響評価 (SIR) : 高

CVSS ベーススコア : 7.2

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

CVE-2026-76425: Cisco ISE SQLインジェクションの脆弱性

Cisco ISEのAPIの脆弱性により、認証されたりリモートの攻撃者がバックエンドデータベースに対してSQLインジェクション攻撃を実行できる可能性があります。

この脆弱性は、SQLクエリに直接連結される特定のパラメータの検証が不十分であることに起因します。攻撃者は、SQL文を含む巧妙に細工された要求を該当エンドポイントに送信することで、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SQLデータベースから任意のコンテンツを読み取り、サーバ側の要求フォージェリ(SSRF)攻撃を実行できる可能性があります。この脆弱性をエクスプロイトするには、攻撃者は有効な管理者ログイン情報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: [CSCwu26054](#)

CVE ID : CVE-2026-76425

セキュリティ影響評価 (SIR) : 高

CVSS ベーススコア : 7.6

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

CVE-2026-76426: Cisco ISE REST APIのSQLインジェクションの脆弱性

Cisco ISEおよびCisco ISE-PICのREST APIの脆弱性により、認証されたりリモートの攻撃者がモニタリングデータベースに対してSQLインジェクション攻撃を実行できる可能性があります。

この脆弱性は、SQL文に連結される特定のパラメータの検証が不十分であることに起因します。攻撃者は、該当パラメータの1つにSQL文が含まれている要求を巧妙に細工して送信することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者はモニタリングデータベースから情報を読み取る可能性があります。この脆弱性をエクスプロイトするには、攻撃者は有効な管理者ログイン情報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: [CSCwu20156](#)

CVE ID : CVE-2026-76426

セキュリティ影響評価 (SIR) : 中

CVSS ベーススコア : 4.9

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

CVE-2026-76427: Cisco ISE XML外部エンティティインジェクションの脆弱性

Cisco ISEのオフラインプロファイラフィードサービスの脆弱性により、認証されたりリモートの攻撃者が、該当デバイスに保存されている任意のファイルを読み取る可能性があります。

この脆弱性は、外部エンティティの解決を無効にしないXMLパーサーを使用した、攻撃者によって制御されるフィードメタデータの解析に起因します。攻撃者は、管理インターフェイスを介して巧妙に細工されたオフラインフィードパッケージをアップロードすることにより、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、攻撃者はファイルシステムから任意のファイルを読み取り、該当デバイスから内部システムに要求を発行できる可能性があります。この脆弱性をエクスプロイトするには、攻撃者は有効な管理者ログイン情報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: [CSCwu27428](#)

CVE ID : CVE-2026-76427

セキュリティ影響評価 (SIR) : 中

CVSS ベーススコア : 4.9

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

CVE-2026-76428: Cisco ISEプロファイラのSQLインジェクションの脆弱性

Cisco ISEおよびCisco ISE-PICのREST APIの脆弱性により、認証されたりリモート攻撃者がセッションデータベースに対してSQLインジェクション攻撃を実行できる可能性があります。

この脆弱性は、パラメータ化を使用せずに特定のパラメータをSQL句に直接連結することに起因します。攻撃者は、該当パラメータの1つにSQL文が含まれている要求を巧妙に細工して送信する

ことで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者はセッションデータベースから情報を読み取る可能性があります。この脆弱性をエクスプロイトするには、攻撃者は有効な管理者ログイン情報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: [CSCwu43502](#)
CVE ID : CVE-2026-76428
セキュリティ影響評価 (SIR) : 中
CVSS ベーススコア : 4.9
CVSS ベクトル : CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/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

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

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。中央と右側の列は、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最初のリリースを示しています。このセクションの表に記載されている適切な [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	CVE-2026-76423 の最初の修正済みリリース	CVE-2026-76424、CVE-2026-76425、CVE-2026-76426、CVE-2026-76427、およびCVE-2026-76428の最初の修正済みリリース
3.1	3.1 パッチ 12	修正済みリリースに移行。
3.2	3.2 パッチ 11	修正済みリリースに移行。
3.3	3.3 パッチ 12	3.3 パッチ 12
3.4	3.4 パッチ 7	3.4 パッチ 7
3.51	3.5 パッチ 4	3.5 パッチ 4

1. 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

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

シスコは、これらの脆弱性を報告していただいたSTAR Labs SG Pte. LtdのLi Jiantao氏とTevel Sho氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-hrP9jQSQ>

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。