Cisco Identity Services Engineの認証されたリモートコード実行およびAPIの脆弱性

Advisory ID : cisco-sa-ise-mult-vul-ymSsTLCc
初公開日 : 2026-09-16 16:00
バージョン 1.0 : Final
CVSSスコア : 9.1
回避策 : Yes
Cisco Bug ID : CSCwu31070 CSCwu40000 CSCwu66592

CVE-2026-20282
CVE-2026-20283
CVE-2026-20284

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)の複数の脆弱性により、認証されたリモートの攻撃者が、該当デバイスの基盤となるオペレーティングシステムでSQLインジェクションを実行したり、データを変更したり、任意のコマンドを実行したりす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。

注：CVE-2026-20282およびCVE-2026-20283について、シスコはスコアの示すとおりMediumではなくHighのSecurity Impact Rating(SIR)を設定しました。これは、達成された特権レベルからrootへ容易に到達できるためです。

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があります。

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-mult-vul-ymSsTLCc

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-2026-20284:SXPサービスが有効になっていて、少なくとも1つのSXP接続が設定されている場合、この脆弱性はCisco ISEに影響します。

CVE-2026-20283：この脆弱性は、複数のネットワークインターフェイスが存在し、そのうちの少なくとも1つがCisco ISEと物理ネットワークアクセスデバイス(NAD)の間のアクティブIPsecトンネルとして設定されている場合、Cisco ISEに影響を与えます。

CVE-2026-20282：この脆弱性は、デバイス設定に関係なく、Cisco ISE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。

SXP設定の確認

SXPサービスが有効になっているかどうかを確認するには、次の手順を実行します。

1. Administration > System > Deployment > Deploymentの順に選択します。
2. チェックするノードをクリックします。
3. Policy Serviceのセクションで、Enable SXP Serviceの設定を確認します。

サービスが有効になっている場合、ノードには脆弱性のある設定が含まれています。

注：各ノードをオンにする必要があります。

SXP接続が設定されているかどうかを確認するには、Work Centers > TrustSec > SXP > SXP Devicesの順に選択してデバイスを確認します。

- デバイスがリストされている場合、ノードには脆弱性のある設定が含まれています。
- デバイスが表示されない場合、ノードには脆弱性のある設定はありません。

IPSecトンネル設定の判別

IPSecトンネルが設定されているかどうかを確認するには、Administration > System > Settings > Protocols > IPSec > Native IPSecの順に選択して、エントリを確認します。

エントリがない場合、デバイスには脆弱性のある設定はありません。

エントリがある場合は、NAD IPアドレスを確認します。

- IPアドレスまたは完全修飾ドメイン名(FQDN)のみが設定されている場合、デバイスには脆弱性のある設定はありません。
- フィールドに他の値が表示されている場合、そのデバイスには脆弱性のある設定が含まれ

ています。

Configure VTIボックスにチェックマークが入っている場合は、Remote and Local Tunnel IPアドレスを確認します。

- IPアドレスまたはFQDNのみが設定されている場合、デバイスには脆弱性のある設定はありません。
- フィールドに他の値が表示されている場合、そのデバイスには脆弱性のある設定が含まれています。

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。

これらの脆弱性が 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。

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-2026-20284:Cisco ISE SXP REST APIのSQLインジェクションの脆弱性

Cisco ISEのSXP REST APIの脆弱性により、認証されたリモート攻撃者が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、REST APIコールでの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、巧妙に細工された入力を該当デバイスに送信することにより、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の基盤となるデータベースのデータを表示または変更できる可能性があります。シングルノード導入では、この脆弱性の不正利用に成功すると、影響を受けるISEノードが使用できなくなり、DoS状態が発生する可能性があります。この状態では、まだ認証されていないエンドポイントは、ノードが復元されるまでネットワークにアクセスできません。

この脆弱性を不正利用するには、攻撃者は有効な管理クレデンシャルを持ち、SXPサービスを有効にし、少なくとも1つのSXP接続を設定し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: CSCwu66592
CVE ID：CVE-2026-20284
セキュリティ影響評価（SIR）：致命的
CVSS ベーススコア：9.1
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CVE-2026-20283:Cisco ISE IPsec Open APIのコマンドインジェクションの脆弱性

Cisco ISEのIPsec Open APIエンドポイントにおける脆弱性により、認証されたリモートの攻撃者が、基盤となるオペレーティングシステムに任意のコマンドを挿入できる可能性があります。

この脆弱性は、IPSec Open APIコールにおけ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、巧妙に細工された入力を該当デバイスのIPsec Open APIエンドポイントに送信することにより、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、攻撃者は基盤となるオペレーティングシステムで任意のコマンドを実行できる可能性があります。

この脆弱性を不正利用するには、攻撃者が有効な管理クレデンシャルを持ち、ノードが複数のネットワークインターフェイスを持つ必要があります。そのインターフェイスの1つは、アクティブなIPSecトンネルとして設定されている必要があります。

注：CVE-2026-20283に関して、シスコはスコアが示すセキュリティ影響評価(SIR)を中よりも高に設定しました。これは、達成された特権レベルからrootへ容易に到達できるためです。

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。本脆弱性に対処する回避策がいくつかあります。

バグID: CSCwu31070
CVE ID：CVE-2026-20283
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：6.5
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N

CVE-2026-20282:Cisco ISE認証書き込みの脆弱性

Cisco ISEの脆弱性により、認証されたリモートの攻撃者が、該当デバイスの基盤となるオペレーティングシステムへの書き込みアクセス権を取得できる可能性があります。

この脆弱性は、ユーザ指定の入力の検証が不十分であることに起因します。攻撃者は、該当デバイスに巧妙に細工された HTTP 要求を送信することにより、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、攻撃者は基盤となるオペレーティングシステムへの書き込みアクセス権を取得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。

注：CVE-2026-20282に関して、シスコはスコアが示すセキュリティ影響評価(SIR)を中よりも高に設定しました。これは、達成された特権レベルからrootへ容易に到達できるためです。

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: CSCwu40000
CVE ID：CVE-2026-20282
セキュリティ影響評価（SIR）：高
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:N/I:H/A:N

回避策

CVE-2026-20282およびCVE-2026-20284：これらの脆弱性に対処する回避策はありません。

CVE-2026-20283：この脆弱性に対処する回避策があります。この脆弱性は、APIを使用してIPsec VTIトンネルが作成された場合にのみ存在します。ただし、Cisco ISE Webインターフェイスを使用してIPsec VTIトンネルを作成しても、脆弱性を設定することはできません。

脆弱な設定が存在する場合は、次の手順を実行します。

1. Administration > System > Settings > Protocols > IPsec > Native IPsecの順に選択します。
2. 脆弱な設定が含まれているトンネルを選択して削除します。
3. Webインターフェイスを使用してトンネルを追加し直します。

この回避策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

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。残りの列には、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最初のリリースが示されます。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 リリース	First Fixed Release（修正された最初のリリース）CVE-2026-20284の場合	First Fixed Release（修正された最初のリリース）CVE-2026-20283の場合	First Fixed Release（修正された最初のリリース）CVE-2026-20282の場合
3.1 以前	3.1 パッチ 12	脆弱性なし	修正済みリリースに移行。
3.2	3.2 パッチ 11	脆弱性なし	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	3.3 パッチ 12
3.4	3.4 パッチ 7	3.4 パッチ 7	3.4 パッチ 7
3.5	3.5 パッチ 4	3.5 パッチ 4	3.5 パッチ 4

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た脆弱性の公式発表があることを認識しています。

Cisco PSIRT では、このアドバイザリに記載されている脆弱性のいかなる悪用も認識していません。

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-mult-vul-ymSsTLCc

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。