Cisco Identity Services エンジンで認証がバイパスされる脆弱性

Advisory ID : cisco-sa-ISE-ABP-VNSW7Tn5 CVE-2026-76460
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 : CSCww39530

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認証をバイパスできる可能性があります。

この脆弱性は、APIエンドポイントでの認証制御が不十分であることに起因します。攻撃者は、該当するAPIエンドポイントに巧妙に細工された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Webベースの管理インターフェイスをバイパスすることで、該当デバイスへの不正アクセスを取得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。

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-ABP-VNSW7Tn5

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

この脆弱性は、デバイス設定に関係なく、Cisco ISEおよびCisco ISE Passive Identity Connector(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のあ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。

セキュリティ侵害の痕跡

この脆弱性の不正利用が試みられたことを確認するには、access.logを確認し、疑わしいユーザ名を探します。デバイスが分散導入の一部である場合は、各ノードのログを確認します。次に、ログ内で疑わしいユーザ名がどのように検出されるかを示す例を示します。

```
admin#show logging application ise-kong/access.log | include dummyuser
```

その他のaccess.logファイルを表示するには、include debug logsを選択した状態でサポートバンドルを収集し、共有キーの暗号化を使用します。次に、復号化して./ise/logs/apigateway/access.log.<date>.gzでアクセスログを見つけます。

出力にエントリが存在する場合は、悪意のあるアクティビティを示している可能性があります。これは、導入環境内のすべてのノードで実行する必要があります。悪意のあるアクティビティが疑われる場合は、影響を受けるノードを再イメージングし、必要に応じて設定バックアップから復元することを強くお勧めします。

注：この脆弱性の不正利用に成功すると、脅威アクターはルート権限でコマンドを実行できるようになります。このアクセスレベルにより、悪用の証拠や侵害の痕跡が攻撃者によって削除されたり、隠されたりする可能性があります。シスコでは、管理者が影響を受けるデバイスの外部でネットワークログとファイアウォールログを相互チェックして、疑わしいアクティビティを特定することを強く推奨します。疑わしいアクティビティには、影響を受けるデバイスから外部IPアドレスへの予期しないアップロードや、悪意のあるIPアドレスからのダウンロードなどがあります。

回避策

この脆弱性に対処する回避策はありません。ただし、緩和策があります。脆弱性のリモートエクスプロイトを防ぐには、インフラストラクチャ アクセス制御リスト（iACL）を使用して、該当デバイス宛ての必須の管理およびコントロール プレーン トラフィックのみを許可します。

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の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	First Fixed Release（修正された最初のリリース）
3.1	3.1 パッチ 12
3.2	3.2 パッチ 11
3.3	3.3 パッチ 12
3.4	3.4 パッチ 7
3.51	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。この脆弱性の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。

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、この脆弱性が活発に悪用されていることを認識しています。この脆弱性が修正済みのソフトウェアリリースにアップグレードすることを強くお勧めします。

出典

この脆弱性は Cisco Cisco Technical Assistance Center（TAC）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-ISE-ABP-

VNSW7Tn5

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。