Cisco Identity Services Engine のリモートコード実行の脆弱性

Advisory ID : cisco-sa-ise-rce-se7bYU57
初公開日 : 2026-09-16 16:00
バージョン 1.0 : Final
CVSSスコア : 9.9
回避策 : No workarounds available
Cisco Bug ID : CSCws25575 CSCwu26102 CSCwu59400

CVE-2026-20307
CVE-2026-20211
CVE-2026-20176

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任意のコマンドを実行する可能性があります。これら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。

これらの脆弱性の詳細については、このアドバイザリの「詳細情報」の項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-rce-se7bYU57

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

これらの脆弱性は、デバイスの設定に関係なく、Cisco ISE 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。また、これらの脆弱性のいずれかに該当するソフトウェアリリースでも、他の脆弱性には該当しない可能性があります。

脆弱性の詳細は以下のとおりです。

CVE-2026-20307：Cisco ISE のリモートコード実行の脆弱性

Cisco ISEのWebベース管理インターフェイスにおける脆弱性により、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、攻撃者は少なくとも権限の低い管理者クレデンシャルを持っている必要があります。

この脆弱性は、ユーザーが提供した Java バイトストリームが安全に逆シリアル化されないことに起因します。攻撃者は、巧妙に細工されたシリアル化された Java オブジェクトを該当デバイスの Web ベース管理インターフェイスに送信することにより、この脆弱性をエクスプロイトする可能性があります。エクスプロイトが成功すると、攻撃者はデバイス上で任意のコードを実行し、権限をルートに昇格させることができます。シングルノード デプロイメントでは、この脆弱性のエクスプロイトが成功すると、影響を受ける ISE ノードが使用不能になり、サービス妨害（DoS）状態に陥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。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: CSCws25575
CVE ID：CVE-2026-20307
セキュリティ影響評価（SIR）：致命的
CVSS ベーススコア：9.9
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVE-2026-20176：Cisco ISE のリモートコード実行の脆弱性

Cisco ISEの脆弱性により、認証されたリモート攻撃者が、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、攻撃者は有効な高特権の管理者クレデンシャルを持っている必要があります。

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にシステムレベルでアクセスし、権限をrootに昇格できるようになります。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。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: CSCwu26102
CVE ID：CVE-2026-20176
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-2026-20211：Cisco ISE のリモートコード実行の脆弱性

Cisco ISEの脆弱性により、認証されたリモート攻撃者が、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、攻撃者は有効な高特権の管理者クレデンシャルを持っている必要があります。

この脆弱性は、影響を受けるソフトウェアによるJavaオブジェクトの安全でないデシリアライゼーションに起因します。攻撃者は、巧妙に細工されたシリアル化されたJavaオブジェクト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、攻撃者は基盤となるオペレーティングシステムへのユーザーレベルのアクセスを取得してから、ルートに権限を昇格す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。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: CSCwu59400
CVE ID：CVE-2026-20211
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

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。他の3つの列は、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 リリース	の最初の修正済みリリース CVE-2026-20307	の最初の修正済みリリース CVE-2026-20211	の最初の修正済みリリース CVE-2026-20176
3.1 よりも前	修正済みリリースに移行。	修正済みリリースに移行。	脆弱性なし
3.1	3.1パッチ12	3.1パッチ12	脆弱性なし
3.2	3.2パッチ11	3.2パッチ11	3.2パッチ11
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3	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

CVE-2026-20307：この脆弱性を報告していただいたREQON B.V.のJasper Westerman、Yanick de Pater、およびHarm Blankersに感謝いたします。

CVE-2026-20176およびCVE-2026-20211：これらの脆弱性を報告していただいたTrendAI ResearchのJonathan Lein氏に感謝いたします。

CVE-2026-20176：この脆弱性を個別に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-rce-se7bYU57

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。