

Cisco Identity Services Engine認証バイパスの脆弱性



Advisory ID : cisco-sa-ise-multiauth-bypass-[CVE-2026-](#)

[sgD2HbL4](#) [76446](#)

初公開日 : 2026-09-16 16:00 [CVE-2026-](#)

最終更新日 : 2026-09-24 17:16 [76444](#)

バージョン 1.1 : Final [CVE-2026-](#)

CVSSスコア : [5.3](#) [76439](#)

回避策 : No workarounds available [CVE-2026-](#)

Cisco Bug ID : [CSCwu73808](#) [CSCwu73771](#) [76447](#)

[CSCwu73832](#) [CSCwu73786](#)

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、リモート攻撃者によるデータへのアクセスや操作、機密情報の取得、該当デバイスでの証明書やキー関連情報のリロードが可能になる可能性があります。

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-multiauth-bypass-sgD2HbL4>

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-2026-76439：この脆弱性は公開時点で、デバイス設定に関係なくCisco ISEに影響を与えました。

CVE-2026-76444、CVE-2026-76446、およびCVE-2026-76447：これらの脆弱性は、発行時点で、デバイス設定にかかわらずCisco ISEおよびCisco ISE-PICに影響を与えました。

このアドバイザリの公開時点で脆弱性が存在するシスコ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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細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ではなく、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-2026-76439：Cisco ISE のリモートコード実行の脆弱性

Cisco ISEのゲストポータルWebアプリケーションのエンドポイントポスチャステータスレポート機能の脆弱性により、認証されていないリモートの攻撃者が、不正なポスチャステータスイベントをエンドポイントポスチャパイプラインに送信できる可能性があります。

この脆弱性は、ゲストポータルを通じて公開される内部インターフェイスでの認証が不十分であることに起因します。攻撃者は、該当システム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、攻撃者は該当システムのポスチャステータスを操作できる可能性があります。

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: [CSCwu73771](#)

CVE ID：CVE-2026-76439

セキュリティ影響評価（SIR）：中

CVSS ベーススコア：5.3

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

CVE-2026-76444: Cisco ISEの情報開示の脆弱性

Cisco ISEおよびCisco ISE-PICの内部サービスの脆弱性により、認証されていないリモートの攻撃者が該当デバイスから機密の設定情報を取得する可能性があります。

この脆弱性は、Policy Runtime Repository Table(PRRT)サービスでの認証の欠落に起因します。細工された要求が該当デバイスに送信されると、この脆弱性がエクスプロイトされる危険性があります。エクスプロイトに成功すると、攻撃者は影響を受けるデバイスから機密の設定情報を取得できる可能性があります。

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: [CSCwu73786](#)

CVE ID : CVE-2026-76444

セキュリティ影響評価 (SIR) : 中

CVSS ベーススコア : 5.3

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

CVE-2026-76447: Cisco ISE証明書リロードの脆弱性

Cisco ISEおよびCisco ISE-PICのOnline Certificate Status Protocol(OCSP)レスポндаの脆弱性により、認証されていないリモートの攻撃者がOCSPレスポнда証明書およびキー関連情報の管理リロードを引き起こす可能性があります。

この脆弱性は、OCSPレスポндаの機能で認証が欠落していることに起因します。細工された要求が該当デバイスに送信されると、この脆弱性がエクスプロイトされる危険性があります。不正利用に成功すると、攻撃者はOCSPレスポндаに証明書とキー情報をオンデマンドでリロードさせる可能性があります。

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: [CSCwu73832](#)

CVE ID : CVE-2026-76447

セキュリティ影響評価 (SIR) : 中

CVSS ベーススコア : 5.3

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

CVE-2026-76446: Cisco ISE外部エンティティインジェクションの脆弱性

Cisco ISEおよびCisco ISE-PICのAPIにおける脆弱性により、認証されたりリモートの攻撃者が、該当デバイスの基盤となるオペレーティングシステム上の特定のファイルを読み取る可能性があります。

この脆弱性は、XML外部エンティティ参照の不適切な制限に起因します。細工された要求が該当デバイスに送信されると、この脆弱性がエクスプロイトされる危険性があります。エクスプロイ

トに成功すると、攻撃者は、影響を受けるシステム上で、基盤となるプロセスがアクセス許可を持つ特定のファイルを読み取る可能性があります。

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: [CSCwu73808](#)
CVE ID : CVE-2026-76446
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。

修正リリース

発行時点では、次の表に示すリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左の列にはシスコのソフトウェアリリースが、中央の列と右の列には、その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と、これらの脆弱性に対する修正を含むリリースが示されています。

Cisco ISE または ISE-PIC リリース	CVE-2026-76439、CVE-2026-76446、および CVE-2026-76447の最初の修正済みリリース	CVE-2026-76444 の最初の修正済みリリース
3.2 以前	修正済みリリースに移行。	脆弱性なし
3.3	3.3パッチ12	脆弱性なし
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次の方々に感謝いたします。

- STAR Labs SG Pte. LtdのLi JiantaoおよびTevel Sho:CVE-2026-76439、CVE-2026-76444、CVE-2026-76446、CVE-2026-76447
- Nicholas Kloster、独立セキュリティ研究者：CVE-2026-76447

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multiauth-bypass-sgD2HbL4>

改訂履歴

バージョン	説明	セクション	Status	日付
1.1	研究者を追加。	送信元	Final	2026年9月24日
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。