

Cisco Identity Services Engineの複数のパストラバーサルの脆弱性



Advisory ID : cisco-sa-ise-multi-traversal-WDTgYCdn [CVE-2026-76434](#)
初公開日 : 2026-09-16 16:00 [CVE-2026-76433](#)
バージョン 1.0 : Final [CVE-2026-76432](#)
CVSSスコア : [5.3](#) [CVE-2026-76431](#)
回避策 : No workarounds available
Cisco Bug ID : [CSCwu73781](#) [CSCwu73783](#) [CSCwu73778](#) [CSCwu73820](#)

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にパストラバーサル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-traversal-WDTgYCdn>

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

公開時点で、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。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-2026-76433: Cisco ISEの情報開示の脆弱性

Cisco ISEおよびCisco ISE-PICのクライアントプロビジョニングダウンロード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該当デバイスの保護されたファイルにアクセスできる可能性があります。

この脆弱性は、ソフトウェアがプロビジョニングリソース要求を処理するときに、ユーザ指定のパスのディレクトリトラバーサル文字シーケンスの検証が不十分であることに起因します。攻撃者は、巧妙に細工された要求をプロビジョニングダウンロードサービ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、攻撃者は認証なしで保護されたファイルにアクセスし、機密情報を暴露す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: [CSCwu73783](#)

CVE ID : CVE-2026-76433

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-2026-76431: Cisco ISEの任意のファイル削除の脆弱性

Cisco ISEおよびCisco ISE-PICのWebベース管理インターフェイスのファイル管理機能における

脆弱性により、認証されたりモートの攻撃者が該当デバイス上の任意のファイルとディレクトリを削除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。

この脆弱性は、要求を検証する前に、ユーザ指定のファイルパスでディレクトリトラバーサル文字シーケンスの検証が不適切なことに起因します。攻撃者は、該当デバイスの Web ベース管理インターフェイスに巧妙に細工されたリクエストを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。エクスプロイトに成功すると、攻撃者は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で任意のファイルとディレクトリを削除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: [CSCwu73778](#)

CVE ID : CVE-2026-76431

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:N/I:H/A:N

CVE-2026-76432: Cisco ISEの任意のファイルへの書き込みの脆弱性

Cisco ISEおよびCisco ISE-PICのWebベースの管理インターフェイスにおける脆弱性により、管理レベル権限を持つ認証されたりモートの攻撃者が、該当デバイスに任意のファイルを書き込む可能性があります。

この脆弱性は、アップロードプロセス中に、該当ソフトウェアがユーザ指定のファイルパスのディレクトリトラバーサル文字シーケンスを正しく検証しないことに起因しています。攻撃者が、巧妙に細工されたファイルに影響を受けるシステムにアップロードしてこの脆弱性をエクスプロイトすることも考えられます。エクスプロイトに成功すると、攻撃者は該当システムの任意の場所にファイルを書き込むことができます。

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: [CSCwu73781](#)

CVE ID : CVE-2026-76432

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:N/I:H/A:N

CVE-2026-76434: Cisco ISEの任意のファイル読み取りの脆弱性

Cisco ISEおよびCisco ISE-PICのWebベース管理インターフェイスの証明書インポート機能にお

ける脆弱性により、認証されたりモート攻撃者が該当システムから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。

この脆弱性は、該当する機能によ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、該当デバイスの Web ベース管理インターフェイスに巧妙に細工されたリクエストを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。エクスプロイトに成功すると、攻撃者は影響を受けるデバイスから機密情報を含む任意のファイルを読み取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: [CSCwu73820](#)
CVE ID : CVE-2026-76434
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

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。

左の列にはシスコソフトウェアリリースが、右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リリースが示されています。

Cisco ISEまたはISC-PICリリース	First Fixed Release (修正された最初のリリース)
3.1	修正済みリリースに移行。
3.2	修正済みリリースに移行。
3.3	3.3 パッチ 12

Cisco ISEまたはISC-PICリリース	First Fixed Release (修正された最初のリリース)
3.4	3.4 パッチ 7
3.51	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-traversal-WDTgYCdn>

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。