

Cisco Identity Services Engine 802.1Xのセッションハイジャックと情報開示の脆弱性



Advisory ID : cisco-sa-ise-multi-vuln-kWLeNnRD

初公開日 : 2026-09-16 16:00

バージョン 1.0 : Final

CVSSスコア : [4.9](#)

回避策 : No workarounds available

Cisco Bug ID : [CSCwp98022](#) [CSCwp98024](#)

[CVE-2026-20071](#)

[CVE-2026-20072](#)

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、認証されていないローカルの攻撃者が認証バイパスを実行したり、機密情報を開示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。

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-vuln-kWLeNnRD>

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。

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、他の脆弱性をエクスプロイトする必要はありません。また、いずれかの脆弱性の影響を受ける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-2026-20072: Cisco ISE の情報開示の脆弱性

Cisco ISE の Web ベース管理インターフェイスの脆弱性により、認証されたリモートの攻撃者が、攻撃者が割り当てられているセキュリティグループ外のネットワークユーザから機密情報を取得できる可能性があります。

この脆弱性は、特定のファイルに適切な許可が適用されないことに起因します。ネットワークユーザに対する管理者権限と管理権限を持つ攻撃者が、ユーザをエクスポートすることにより、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、通常は管理者に見えないパスワードを表示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: [CSCwp98024](#)

CVE ID : CVE-2026-20072

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

CVE-2026-20071: Cisco ISE セッションテイクオーバーの脆弱性

Cisco ISE の SSID 個人所有デバイス持ち込み (BYOD) オンボーディングワークフローにおける脆弱性により、認証されていない隣接する攻撃者が別のユーザのオンボーディングセッションを乗っ

取り、保護された802.1Xネットワークにアクセスする可能性があります。

この脆弱性は、ユーザのオンボーディング中に実行される認証チェックが不十分であることに起因します。攻撃者は、正当なユーザをスプーフィングしてゲストWebポータルへのリダイレクトをトリガーすることにより、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者はユーザセッションを引き継ぎ、保護された802.1Xネットワークにアクセス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: [CSCwp98022](#)
CVE ID : CVE-2026-20071
SIR : 中
CVSS ベーススコア : 3.8
CVSSベクトル : CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:C/C:N/I:L/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表示されます。中央と右側の列には、リリースがこれらの脆弱性の影響を受けたかどうか、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ています。

Cisco ISE リリース	CVE-2026-20071 の最初の修正済みリリース	CVE-2026-20072 の最初の修正済みリリース
3.1 以前	修正済みリリースに移行。	修正済みリリースに移行。
3.2	修正済みリリースに移行。	3.2 パッチ 8
3.3	3.3 パッチ 12	3.3 パッチ 8
3.4	3.4 パッチ 7	3.4 パッチ 7

Cisco ISE リリース	CVE-2026-20071 の最初の修正済みリリース	CVE-2026-20072 の最初の修正済みリリース
3.5	3.5 パッチ 4	3.5 パッチ 3

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

シスコは、これらの脆弱性を報告していただいたAbacus社のDennis Carlson氏とAndres Lara氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-vuln-kWLeNnRD>

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。