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

Medium

アドバイザリーID : cisco-sa-ise-unauth-bypass-uxjRXGpb
初公開日 : 2026-05-06 16:00
バージョン 1.0 : Final
CVSSスコア : 5.3
回避策 : No workarounds available
Cisco バグ ID : CSCwr77445 CSCwr77441

CVE-2026-20195
CVE-2026-20193

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

Cisco Identity Services Engine(ISE)の複数の脆弱性により、リモート攻撃者が認可メカニズムをバイパスしたり、エラーメッセージを調査して該当デバイスの機密情報にアクセス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-unauth-bypass-uxjRXGpb

該当製品

脆弱性のある製品

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、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-2026-20195:Cisco ISEで確認できる応答不一致の脆弱性

Cisco ISEのアイデンティティ管理APIエンドポイントにおける脆弱性により、認証されていないリモートの攻撃者が、該当デバイスの有効なユーザアカウントを列挙できる可能性があります。

この脆弱性は、影響を受けるAPIエンドポイントが呼び出されたときにエラーメッセージが表示されることに起因します。攻撃者は、巧妙に細工された一連の要求を該当のエンドポイントに送信し、差別化された応答を分析することで、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有効なユーザ名のリストをコンパイル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: CSCwr77445
CVE ID：CVE-2026-20195
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-2026-20193:Cisco ISE認証バイパスの脆弱性

Cisco ISEのRADIUSポリシーAPIエンドポイント(API)の脆弱性により、読み取り専用の管理者権限を持つ認証されたリモートの攻撃者が、該当デバイスの機密情報に不正アクセスする可能性があります。

この脆弱性は、RADIUSポリシーAPIエンドポイントでの不適切なロールベースアクセスコントロール(RBAC)権限に起因します。攻撃者は、Webベースの管理インターフェイスをバイパスし、影響を受けるエンドポイントを直接呼び出すことで、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、各自のロールに対して制限されているRADIUSポリシーの機密情報への不正な読み取り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。

バグID: CSCwr77441
CVE ID：CVE-2026-20193
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.3
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/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。これらの脆弱性を完全に修正し、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。

Cisco ISE リリース	First Fixed Release（修正された最初のリリース）
3.2 以前	修正済みリリースに移行。
3.3	3.3 パッチ 11
3.4	3.4 パッチ 6
3.5	3.5 パッチ 3
3.6	脆弱性なし

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

これらの脆弱性を報告してくださった外部調査員の方に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-bypass-uxjRXGpb

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5月6日

利用規約

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。