Cisco Identity Services エンジンで承認がバイパスされる脆弱性

Medium

アドバイザリーID : cisco-sa-ise-auth-bypass-mVfKVQAU
初公開日 : 2025-06-25 16:00
バージョン 1.0 : Final
CVSSスコア : 6.4
回避策 : No workarounds available
Cisco バグ ID : CSCwm59423

CVE-2025-20264

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特定の管理機能の認証メカニズムをバイパスできる可能性があります。

この脆弱性は、外部IDプロバイダーとのSAML SSO統合によって作成されたユーザの権限適用メカニズムが不十分であることに起因します。攻撃者は、一連の特定のコマンドを該当デバイスに送信することで、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、システムの再起動を引き起こす可能性のある一部のシステム設定を含め、限られた数のシステム設定を変更できる可能性があります。シングルノードのCisco ISE導入では、ネットワークで認証されていないデバイスは、Cisco ISEシステムがオンラインに戻るまで認証できません。

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。

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-auth-bypass-mVfKVQAU

該当製品

脆弱性のある製品

この脆弱性は、公開時点で、ユーザ作成に外部アイデンティティプロバイダーとのSAML SSO統合を使用した場合に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。

脆弱性が Cisco ISE Passive Identity Connector に影響しないことはシスコで確認済みです。

回避策

こ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

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手でき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完全なアップグレード ソリューション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。

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。このアドバイザリの先頭にあるバグ IDの詳細情報のセクションで、最新の情報を確認してください。

左側の列にはシスコソフトウェアリリース、右側の列に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 リリース	First Fixed Release（修正された最初のリリース）
3.1 以前	修正済みリリースに移行。
3.2	3.2P8（2025年11月）
3.3	3.3P5
3.4	3.4P2

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やその公表は確認しておりません。

出典

この脆弱性を報告していただいたToyotaのJesse Via氏に感謝いたします。

URL

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

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	2025年6月25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。