Cisco Identity Services EngineのRADIUS抑制におけるDoS脆弱性

High

アドバイザリーID : cisco-sa-ise-radsupress-dos-8YF3JThh
初公開日 : 2025-11-05 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : Yes
Cisco バグ ID : CSCwq27605

CVE-2025-20343

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)で障害が繰り返し発生するクライアントからのRADIUS要求を拒否するReject RADIUS設定の脆弱性により、認証されていないリモートの攻撃者がCisco ISEの予期しない再起動を引き起こす可能性があります。

この脆弱性は、すでに拒否されたエンドポイントであるMACアドレスに対するRADIUSアクセス要求を処理する際の論理エラーが原因で発生します。攻撃者は、巧妙に細工された複数のRADIUSアクセス要求メッセージの特定のシーケンスをCisco ISE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、Cisco ISEの再起動時にサービス拒否(DoS)状態が引き起こされる危険性があります。

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。本脆弱性に対処する回避策がいくつかあります。

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-radsupress-dos-8YF3JThh

該当製品

脆弱性のある製品

この脆弱性は、Cisco ISEリリース3.4.0、3.4パッチ1、3.4パッチ2、および3.4パッチ3で、デフォルトで繰り返し失敗するクライアントからのRADIUS要求を拒否する設定が有効になっています。

脆弱性のある Cisco ソフトウェアリリースの詳細については、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。

デバイス設定の確認

Reject RADIUS requests from clients with repeat failuresが有効になっているかどうかを確認するには、Cisco ISE Web UIでAdministration > System > Settings > Protocols > RADIUSの順に選択します。「繰り返し失敗したクライアントと繰り返しアカウンティングを抑制する」セクションに移動します。この設定を有効にするチェックボックスは、デフォルト設定であるためオンにする必要があります。

Cisco ISEリリース3.4.0で新しく導入されたこの機能の詳細については、『Cisco Identity Services Engine管理者ガイド、リリース3.4』の「RADIUSの設定」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（ISE-PIC）に影響しないことはシスコで確認済みです。

回避策

Cisco ISEデバイスは、繰り返し障害が発生するクライアントからのRADIUS要求を拒否するが設定されている場合にのみ、この脆弱性の影響を受けます。

回避策として、管理者は次の手順を使用してこの設定を無効にすることができます。

1. Administration > System > Settings > Protocols > RADIUSの順に選択します。
2. 「繰り返し失敗したクライアントと繰り返しアカウンティングを抑制する」セクションに移動します。
3. Reject only RADIUS requests from clients with repeat failuresチェックボックスのチェックマークを外します。

この設定はデフォルトで有効になっており、ほとんどの環境で設定されます。この設定を無効にした場合、Cisco ISEデバイスはこの脆弱性の影響を受けません。ただし、デバイスを修正コードにアップグレードした後で、この構成設定を再度有効にすることを推奨します。

Cisco ISEリリース3.4.0で新しく導入されたこの機能の詳細については、『Cisco Identity Services Engine管理者ガイド、リリース3.4』の「RADIUSの設定」を参照してください。

この回避策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策また

は緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

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

次の表に示すように、該当する修正済みのソフトウェア リリースにアップグレードすることをお勧めします。

Cisco ISE リリース	First Fixed Release（修正された最初のリリース）
3.3 以前	脆弱性なし
3.4	3.4 パッチ 4
3.5	脆弱性なし

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

この脆弱性は Cisco Cisco Technical Assistance Center（TAC）サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-radsupress-dos-8YF3JThh

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11月5日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 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。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、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。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。