Cisco Identity Services Engineのリモートコード実行の脆弱性

アドバイザリーID : cisco-sa-ise-rce-4fverepv
初公開日 : 2026-04-15 16:00
バージョン 1.0 : Final
CVSSスコア : 9.9
回避策 : No workarounds available
Cisco バグ ID : CSCwq21242 CSCwq22993

CVE-2026-20180
CVE-2026-20186

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、認証されたリモートの攻撃者が該当デバイスの基盤となるオペレーティングシステムで任意のコマンドを実行できる可能性があります。これらの脆弱性をエクスプロイトするには、攻撃者は少なくとも読み取り専用(RO)の管理者クレデンシャルを持っている必要があります。

この脆弱性は、ユーザ提供による入力の検証が不十分であることが原因です。攻撃者は、該当デバイスに巧妙に細工されたHTTP要求を送信することにより、これら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、攻撃者は基盤となるオペレーティングシステムへのユーザーレベルのアクセスを取得してから、ルートに権限を昇格する可能性があります。シングルノードCisco ISEの導入では、これらの脆弱性の不正利用に成功すると、影響を受けるISEノードが使用不能になり、サービス拒否(DoS)状態が発生する可能性があります。この状態では、まだ認証されていないエンドポイントは、ノードが復元されるまでネットワークにアクセスできません。

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-rce-4fverepv

該当製品

脆弱性のある製品

これらの脆弱性は、デバイスの設定に関係なく、Cisco ISEに影響します。

脆弱性が存在する Cisco 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。

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。

シスコは、これらの脆弱性がCisco ISE Passive Identity Connector(ISE-PIC)には影響を与えないことを確認しました。

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

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。右の列は、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、およびこれらの脆弱性に対する修正を含む最初のリリースを示しています。このセクションの表に記載されている適切な修正済み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）
3.2 より前	修正済みリリースに移行。
3.2	3.2 パッチ 8
3.3	3.3 パッチ 8
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とその公表は確認しておりません。

出典

これらの脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のX.B.による社内セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-4fverepv

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4月15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。