Cisco Identity Services Engineのリモートコード実行およびパストラバーサルの脆弱性

アドバイザリーID : cisco-sa-ise-rce-traversal-8bYndVrZ
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 : CSCws52738 CSCws52717

CVE-2026-20147
CVE-2026-20148

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)およびCisco ISE Passive Identity Connector(ISE-PIC)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でリモートコードを実行したり、パストラバーサル攻撃を実行したりする可能性があります。これらの脆弱性を不正利用するには、攻撃者は有効な管理者クレデンシャルを持っている必要があります。

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-rce-traversal-8bYndVrZ

該当製品

脆弱性のある製品

これらの脆弱性は、デバイス設定に関係なく、Cisco ISEおよびCisco ISE-PICに影響を与えます。

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。

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別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェア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-2026-20147:Cisco ISEのリモートコード実行の脆弱性

Cisco ISEおよびCisco ISE-PICの脆弱性により、認証されたリモート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。この脆弱性を不正利用するには、攻撃者は有効な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、ユーザ指定の入力の検証が不十分であることに起因します。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ISE導入では、この脆弱性の不正利用に成功すると、影響を受けるISEノードが使用できなくなり、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: CSCws52738
CVE ID：CVE-2026-20147
セキュリティ影響評価（SIR）：致命的
CVSS ベーススコア：9.9
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVE-2026-20148:Cisco ISEのパストラバーサルの脆弱性

Cisco ISEおよびCisco ISE-PICの脆弱性により、認証されたリモートの攻撃者が、基盤となるオペレーティングシステムに対してパストラバーサル攻撃を実行し、任意のファイルを読み取る可能性があります。この脆弱性を不正利用するには、攻撃者は有効な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、ユーザー入力の検証が不適切なことに起因します。攻撃者は、該当システムに巧

妙に細工された HTTP 要求を送信することにより、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、攻撃者は該当システムの機密ファイル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: CSCws52717
CVE ID：CVE-2026-20148
セキュリティ影響評価（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

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 または ISE-PIC リリース	First Fixed Release（修正された最初のリリース）
3.1 より前	修正済みリリースに移行。
3.1	3.1パッチ11（2026年4月）
3.2	3.2パッチ10（2026年4月）
3.3	3.3パッチ11（2026年4月）
3.4	3.4パッチ6（2026年4月）
3.51	3.5 パッチ 3

1. Cisco ISE-PICは販売終了日に達しています。リリース3.4がサポートされる最後のリリースです。

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TrendAI ResearchのJonathan Lein氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-traversal-8bYndVrZ

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。