

Cisco Identity Services Engineにおけるリモートでのコード実行と情報漏えいの脆弱性



アドバイザーID : cisco-sa-ise-multi-G5WP8vv

[CVE-2026-20181](#)

初公開日 : 2026-06-17 16:00

[CVE-2026-](#)

最終更新日 : 2026-06-19 15:02

[20190](#)

バージョン 1.1 : Final

CVSSスコア : [9.1](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwt22936](#) [CSCwt22913](#)

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、リモート攻撃者が該当デバイスでリモートコードを実行したり、情報漏えい攻撃を実行したりする可能性があります。

これらの脆弱性の詳細については本アドバイザーの「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。

このアドバイザーは、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-multi-G5WP8vv>

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 および Cisco ISE-PIC に影響を及ぼします。

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザーの「[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、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-2026-20181: Cisco ISEおよびISE-PICのリモートコード実行の脆弱性

Cisco ISEおよび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。この脆弱性をエクスプロイトするには、攻撃者は有効な管理者ログイン情報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: [CSCwt22913](#)

CVE ID : CVE-2026-20181

セキュリティ影響評価 (SIR) : 致命的

CVSS ベーススコア : 9.1

CVSSベクトル : CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CVE-2026-20190: Cisco ISEおよびISE-PICの情報開示の脆弱性

Cisco ISEおよびISE-PICの脆弱性により、認証されていないリモートの攻撃者が該当デバイスの機密情報を表示できる可能性があります。

この脆弱性は、リソースにアクセスする際の不適切な認証チェックに起因します。攻撃者は、巧妙に細工されたトラフィックを該当デバイスに送信することによって、本脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者は機密情報（今後の攻撃で使用

される可能性があるハッシュされたクレデンシャルなど)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: [CSCwt22936](#)

CVE ID : CVE-2026-20190

セキュリティ影響評価 (SIR) : 高

CVSS ベーススコア : 7.5

CVSS ベクトル : CVSS:3.1/AV:N/AC:L/PR:N/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。中央および右の列は、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	CVE-2026-20181 の最初の修正 済みリリース	CVE-2026-20190 の最初の修正 済みリリース
3.3 より前	修正済みリリースに移行。	脆弱性なし
3.3	3.3 パッチ 11	脆弱性なし
3.4	3.4 パッチ 6	3.4 パッチ 6
3.51,2	3.5 Patch 4 (2026年8月) また は hot patch	3.5 パッチ 3

1. Cisco ISE- PIC は販売終了日を迎えました。リリース 3.4 が、サポートされる最後のリリースです。

2. Cisco ISEリリース3.5パッチ3のホットパッチは、ご希望に応じて提供されます。[Cisco Technical Assistance Center\(TAC\)](#)にお問い合わせください。

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、CVE-2026-20181を報告していただいたTrendAI ResearchのJonathan Lein氏に感謝いたします。

また、CVE-2026-20181を独自に報告していただいたSTAR Labs SG Pte. Ltd.のLi Jiantao氏とTevel Sho氏にも感謝いたします。

シスコは、CVE-2026-20190を報告していただいたTrendAI Zero Day InitiativeのBobby Gould氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-G5WP8vv>

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	表のホットパッチの提供状況を明確化。	修正済みリリース	Final	2026年6月19日
1.0	初回公開リリース	—	Final	2026年6月17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、単独の転載や意識を施した場合、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。