Cisco Identity Services Engineのクロスサイトスクリプティングと情報漏えいの脆弱性の反映

Medium

アドバイザリーID : cisco-sa-ise-multiple-vulns-O9BESWJH
初公開日 : 2025-11-05 16:00
バージョン 1.0 : Final
CVSSスコア : 5.4
回避策 : No workarounds available
Cisco バグ ID : CSCwo37181 CSCwo37218 CSCwo37216 CSCwo37212

CVE-2025-20304
CVE-2025-20305
CVE-2025-20289
CVE-2025-20303

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機密情報を開示したり、リフレクトされたクロスサイトスクリプティング(XSS)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-multiple-vulns-O9BESWJH

該当製品

脆弱性のある製品

公開時点で、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-2025-20289、CVE-2025-20303、およびCVE-2025-20304:Cisco ISEの反映XSS脆弱性

Cisco ISEおよびCisco ISE-PICのWebベース管理インターフェイスの複数の脆弱性により、認証されたリモートの攻撃者が、インターフェイスのユーザに対してリフレクトXSS攻撃を実行する可能性があります。

これらの脆弱性は、該当システムのWebベース管理インターフェイスでユーザが行った入力の検証が不十分であることに起因します。攻撃者は、悪意のあるコードをインターフェイスの特定のページに挿入することで、これらの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、攻撃者は該当インターフェイスのコンテキストで任意のスクリプトコードを実行したり、ブラウザベースの機密情報にアクセスす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、攻撃者は該当デバイスに少なくとも低特権のアカウントを持っている必要があります。

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。

バグID: CSCwo37212
CVE ID：CVE-2025-20289
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

Bug ID:CSCwo37216およびCSCwo37218
CVE ID：CVE-2025-20303 および CVE-2025-20304
SIR：中
CVSS ベーススコア：5.4
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

CVE-2025-20305:Cisco ISEの情報開示の脆弱性

Cisco 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該当デバイスから機密情報を取得できる可能性があります。

この脆弱性は、特定のファイルに適切なデータ保護メカニズムがないために存在します。読み取り専用のAdministrator権限を持つ攻撃者は、結果が高特権ユーザのみに表示されるアクションを実行することで、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、通常は読み取り専用の管理者には見えないパスワードが攻撃者に表示され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: CSCwo37181
CVE ID：CVE-2025-20305
SIR：中
CVSS ベーススコア：4.3
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/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

発行時点では、次の表に示すリリース情報は正確でした。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。

左の列にはシスコソフトウェアリリースが、右の列にはリリースがこのアドバイザリに記載された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リリースが示されています。

Cisco ISE リリース	CVE-2025-20289 の最初の修正済みリリース	CVE-2025-20303、CVE-2025-20304、およびCVE-2025-20305の最初の修正済みリリース
3.1 以前	修正済みリリースに移行。	修正済みリリースに移行。
3.2	3.2パッチ8（2025年12月）	3.2パッチ8（2025年12月）
3.3	3.3パッチ8（2025年11月）	3.3パッチ8（2025年11月）

Cisco ISE リリース	CVE-2025-20289 の最初の修正済みリリース	CVE-2025-20303、CVE-2025-20304、およびCVE-2025-20305の最初の修正済みリリース
3.4	3.4 パッチ 2	3.4 パッチ 4
3.5	脆弱性なし	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 サポートページにある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

これらの脆弱性を報告していただいたポーランドのING HubsのGrzegorz Misiun氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multiple-vulns-O9BESWJH

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

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。