Cisco Identity Services Engineの認証バイパスとクロスサイトスクリプティングの脆弱性

Medium

アドバイザリーID : cisco-sa-ise-auth-bypass-BBRf7mkE
初公開日 : 2024-11-06 16:00
バージョン 1.0 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCwj28643 CSCwj96002 CSCwj29451

CVE-2024-20537
CVE-2024-20539
CVE-2024-20538

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、リモート攻撃者が該当デバイスのWebベース管理インターフェイスのユーザに対して、許可バイパス攻撃やクロスサイトスクリプティング(XSS)攻撃を実行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-auth-bypass-BBRf7mkE

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に影響を与えました。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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-2024-20537:Cisco ISE認可バイパスの脆弱性

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特定の管理機能の認証メカニズムをバイパスできる可能性があります。

この脆弱性は、サーバ側での管理者権限の検証が不十分であることに起因します。攻撃者は、巧妙に細工されたHTTP要求を該当システムに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、攻撃者は意図したアクセスレベルを超えて管理機能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、読み取り専用の管理者クレデンシャルが必要です。

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:CSCwj28643
CVE ID：CVE-2024-20537
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.5
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N

CVE-2024-20538:Cisco ISEのクロスサイトスクリプティングの脆弱性

Cisco ISEのWebベース管理インターフェイスの脆弱性により、認証されていない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XSS攻撃を実行する可能性があります。

この脆弱性は、Web ベースの管理インターフェイスで、ユーザー入力が適切に検証されないことに起因します。攻撃者は、巧妙に細工されたリンクをクリックするように該当システムのインターフェイスのユーザを誘導することにより、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。

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:CSCwj96002
CVE ID：CVE-2024-20538
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.1
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVE-2024-20539:Cisco ISEストアドのクロスサイトスクリプティングの脆弱性

Cisco ISEのWebベース管理インターフェイスにおける脆弱性により、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ストアドXSS攻撃を実行する可能性があります。

この脆弱性は、Web ベースの管理インターフェイスで、ユーザー入力が適切に検証されないことに起因します。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。この脆弱性をエクスプロイトするには、該当デバイスで有効な管理者クレデンシャルが必要になります。

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:CSCwj29451
CVE ID：CVE-2024-20539
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

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

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性とアップグレード ソリューション一式を確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

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。最新情報については、本アドバイザリ上部のバグ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一覧表示されます。中央と右側の列は、リリースがこれらの脆弱性の影響を受けたかどうか、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。

Cisco ISE リリース	CVE-2024-20537およびCVE-2024-20539の最初の修正済みリリース	CVE-2024-20538 の最初の修正済みリリース
3.0 以前	修正済みリリースに移行。	修正済みリリースに移行。
3.1	3.1P9	3.1P10（2025年1月）
3.2	3.2P7	3.2P7
3.3	3.3P3	3.3P4
3.4	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 Service 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。

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された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

CVE-2024-20537およびCVE-2024-20539：これらの脆弱性は、Cisco TACサポートケースの解決中に発見されました。

CVE-2024-20538：この脆弱性を報告していただいたSTM Cyber社のJakub "kubolos231" Sajniak氏とViet Hoang Nguyen氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-auth-bypass-BBRf7mkE

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	2024年11月6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。