Cisco Identity Services Engine の脆弱性

Medium

アドバイザリーID : cisco-sa-ise-mult-j-KxpNynR
初公開日 : 2023-11-15 16:00
バージョン 1.0 : Final
CVSSスコア : 6.7
回避策 : No workarounds available
Cisco バグ ID : CSCwc45750 CSCwc45768

CVE-2023-20208
CVE-2023-20272

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悪意のあるファイルをアプリケーションのWebルートにアップロードしたり、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。これらの脆弱性を不正利用するには、攻撃者は該当デバイスの有効なログイン情報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-secure-endpoint-dos-RzOgFKnd

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、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-2023-20272:Cisco ISEの任意のファイル書き込みの脆弱性

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悪意のあるファイルをアプリケーションのWebルートにアップロードできる可能性があります。

この脆弱性は、ファイル入力の不十分な検証に起因します。攻撃者は、悪意のあるファイルをWebインターフェイスにアップロードすることにより、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、攻撃者はファイルを置き換え、機密のサーバ側の情報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:CSCwc45768
CVE ID：CVE-2023-20272
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.7
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:L

CVE-2023-20208:Cisco ISE XSS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、該当デバイスのWebベース管理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がユーザ入力を適切に検証しないことに起因しています。攻撃者は、インターフェイスの特定のページに悪意のあるコードを挿入することで、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、攻撃者は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、ブラウザの機密情報にアクセスしたり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、攻撃者は有効な管理者クレデンシャルを必要とします。

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:CSCwc45750
CVE ID：CVE-2023-20208
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、次の表に記載されている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Ciscoソフトウェアリリースがリストされ、中央と右の列には、そのリリースが本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と、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-2023-20272 の最初の修正済みリリース	CVE-2023-20208 の最初の修正済みリリース
2.7 以前	脆弱性なし	脆弱性なし
3.0	3.0P8	3.0P8
3.1	3.1P5	3.1P6
3.2	脆弱性なし	3.2P1
3.3	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。

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

シスコは、これらの脆弱性を報告していただいた次の方々に感謝いたします。

- デロイトのCristian Mocanu氏：CVE-2023-20272およびCVE-2023-20208
- Deloitte社のDan Marin氏、Teodor Cervinski氏、George Jubleanu氏：CVE-2023-20208
- Pear1y:CVE-2023-20272

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-mult-j-KxpNynR

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	2023-NOV-15

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。