Cisco Identity Services Engineの権限昇格の脆弱性

Medium	**アドバイザリーID :** cisco-sa-ise-os-injection-pxhKsDM **初公開日 :** 2023-02-01 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 6.0 **回避策 :** No workarounds available **Cisco バグ ID :** CSCwd07344 CSCwd07341 CSCwd07340	CVE-2023-20022 CVE-2023-20021 CVE-2023-20023

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

特定のCisco Identity Services Engine(ISE)CLIコマンドに複数の脆弱性が存在するため、認証されたローカルの攻撃者が、基盤となるオペレーティングシステムに対してコマンドインジェクション攻撃を実行し、権限を*root*に昇格でき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、攻撃者が該当デバイスに対する有効な*管理者*権限を持っている必要があります。

この脆弱性は、ユーザ提供による入力の検証が不十分であることが原因です。攻撃者は、巧妙に細工されたCLIコマンドを送信することで、これら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 *root* に特権昇格できるようになります。

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。

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-os-injection-pxhKsDM

該当製品

脆弱性のある製品

公開時点では、これらの脆弱性はCisco ISEソフトウェアに影響を及ぼしていました。

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。

シスコは、これらの脆弱性がCisco Evolved Programmable Network Manager(EPNM)およびCisco Prime Infrastructure(PI)には影響を与えないことを確認しました。

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、その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リリースが示されています。

Cisco ISE ソフトウェアリリース	First Fixed Release（修正された最初のリリース）
2.4 以前	脆弱性なし
2.6	脆弱性なし
2.7	脆弱性なし
3.0	脆弱性なし
3.1	脆弱性なし
3.2	3.2P1

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やその公表は確認しておりません。

出典

これらの脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のAndrew Kim氏による内部セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-os-injection-pxhKsDM

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年2月1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。