Cisco IOxアプリケーションホスティング環境の特権昇格の脆弱性

Medium

アドバイザリーID : cisco-sa-rdocker-uATbukKn
初公開日 : 2023-10-04 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 : CSCwf67351

CVE-2023-20235

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 IOS XEソフトウェアのCisco IOxアプリケーションホスティングインフラストラクチャにおけるオンデバイスアプリケーション開発ワークフロー機能の脆弱性により、認証されたリモートの攻撃者が、基盤となるオペレーティングシステムにrootユーザとしてアクセスできる可能性があります。

この脆弱性は、特権ランタイムオプションを持つDockerコンテナがアプリケーション開発モードの場合にブロックされないことに起因します。攻撃者は、Docker CLIを使用して該当デバイスにアクセスすることにより、この脆弱性を不正利用する可能性があります。アプリケーション開発ワークフローは、開発システムでのみ使用することを意図しており、実稼働システムでは使用できません。

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。

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-rdocker-uATbukKn

該当製品

脆弱性のある製品

公開時点では、この脆弱性は、Cisco IOS XEソフトウェアの脆弱性が存在するリリースを実行し、Cisco IOxアプリケーションホスティング環境で設定され、アプリケーション開発ワークフ

ロー機能が有効になっている次のシスコデバイスに影響を与えました。

- Catalyst IE3x00高耐久性シリーズスイッチ
- Catalyst IR1100高耐久性シリーズルータ
- Catalyst IR1800高耐久性シリーズルータ
- Catalyst IR8100ヘビーデューティシリーズルータ
- Catalyst IR8300 高耐久性シリーズ ルータ
- エンベデッドサービス 3300 シリーズ スイッチ

注：Cisco IOS XEソフトウェアリリース17.3.1以降は、アプリケーション開発ワークフロー機能をサポートしています。

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。

アプリケーション開発ワークフロー機能は、デフォルトでは有効になっていません。アプリケーション開発ワークフローは、バイパスによってコンテナを実行できるため、ローカルマネージャやIOx管理アプリケーションには見えません。このため、このワークフローは開発システムでのみ使用することを意図しており、実稼働システムでは使用しません。

アプリケーション開発ワークフローが有効になっているかどうかの確認

アプリケーション開発ワークフローが有効になっているかどうかを確認するには、IOx Local Manager Applicationにログインし、Remote Docker Workflowタブを選択します。Remote Docker Access is enabledが赤で表示されている場合、アプリケーション開発ワークフローは有効になっています。

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、この脆弱性がCisco IC3000産業用コンピューティングゲートウェイには影響を与えないことを確認しました。

回避策

この脆弱性に対処する回避策はありません。

ただし、緩和策として、実稼働環境でアプリケーション開発ワークフロー機能を無効にすることができます。アプリケーション開発ワークフローは、開発システムでのみ使用することを意図しており、実稼働システムでは使用できません。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および

使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

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。

シスコ プラットフォーム	First Fixed Release（修正された最初のリリース）
IOS XEベースのデバイスでIOxが設定されている	17.3.8（2023年10月） 17.6.6 17.9.5（2023年10月） 17.13.1（2023年12月） 詳細については、次のセクションの「Cisco IOSおよびIOS XEソフトウェアチェッカー」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。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの脆弱性による侵害の可能性を判断できるように、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべての脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。あるいは、次のフォームを使用して、シスコ セキュリティ アドバイザリに該当するリリースであるかどうかを確認します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. リリース番号（15.9(3)M2、17.3.3 など）を入力します。
3. [チェック（Check）] をクリックします。

2 | Critical,High,Medium | このアドバイザのみ

Enter release number | Check

不正利用事例と公式発表

Cisco PSIRT は、このアドバイザリで説明されている脆弱性に対してコンセプト実証エクスプロイトコードが利用可能であることを認識しています。

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

出典

この脆弱性を報告していただいたEn Garde Security/ICS RangeリサーチチームのChristian Petersen氏とJens A. Nelsen氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rdocker-uATbukKn

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10月4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、単独の転載や意訳を施した場合、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。