Cisco Evolved Programmable Network ManagerおよびCisco Prime Infrastructureの脆弱性

Medium

アドバイザリーID : cisco-sa-pi-epnm-wkZJeyeq
初公開日 : 2024-01-10 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 : CSCwf81870 CSCwf83557 CSCwf81859 CSCwf83560 CSCwf81865 CSCwf81862 CSCwf83565

CVE-2023-20260
CVE-2023-20271
CVE-2023-20257
CVE-2023-20258

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 Evolved Programmable Network Manager(EPNM)およびCisco Prime Infrastructureの複数の脆弱性により、攻撃者がクロスサイトスクリプティング(XSS)攻撃を実行し、任意のコマンドを実行し、SQLインジェクション攻撃を実行し、または該当システムで昇格された特権を取得する可能性があります。

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。

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。

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-pi-epnm-wkZJeyeq

該当製品

脆弱性のある製品

公開時点で、これらの脆弱性は次のシスコ製品に影響を与えました。

- EPNM
- Prime インフラストラクチャ

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

これらの脆弱性は互いに依存関係があります。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。

Cisco Prime Infrastructureのコマンド実行の脆弱性

Cisco Prime Infrastructure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基盤となるオペレーティングシステムで任意のコマンドを実行する可能性があります。

この脆弱性は、該当アプリケーションによるシリアル化されたJavaオブジェクトの不適切な処理に起因します。アプリケーションの設定を変更するのに十分な権限を持つ攻撃者は、該当アプリケーションで処理される悪意のあるシリアル化されたJavaオブジェクトを含むドキュメントをアップロードすることで、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、攻撃者はアプリケーションに任意のコマンドを実行させ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:CSCwf81859
CVE ID：CVE-2023-20258
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:H/UI:N/S:U/C:H/I:H/A:N

Cisco EPNMおよびCisco Prime InfrastructureのSQLインジェクションの脆弱性

Cisco EPNMおよびCisco Prime Infrastructure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該当システムにSQLインジェクション攻撃を実行する可

能性があります。

この脆弱性は、ユーザーが送信したパラメータの不適切な検証に起因します。攻撃者は、アプリケーションに対して認証を行い、悪意のある要求を該当システムに送信することで、こ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、攻撃者は基盤となるデータベースに保存されている機密情報を取得および変更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:CSCwf81862、CSCwf83557
CVE ID：CVE-2023-20271
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:H/I:N/A:N

Cisco EPNMおよびCisco Prime Infrastructureの権限昇格の脆弱性

Cisco EPNMおよびCisco Prime InfrastructureのアプリケーションCLIの脆弱性により、認証されたローカル攻撃者が昇格された特権を取得する可能性があります。

この脆弱性は、アプリケーションスクリプトへのコマンドライン引数の不適切な処理に起因します。インタラクティブシェルでログインするだけの特権を持つ攻撃者は、悪意のあるオプションを使用してCLIでコマンドを発行することにより、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、攻撃者は基盤となるオペレーティングシステムでrootユーザの昇格した権限を取得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:CSCwf81865、CSCwf83560
CVE ID：CVE-2023-20260
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.0
CVSSベクトル：CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N

Cisco EPNMおよびCisco Prime Infrastructure XSSの脆弱性

Cisco EPNMおよびCisco Prime Infrastructure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に対するユーザ入力の検証が不適切なことに起因します。Webベースの管理インターフェイスにアクセスするのに十分な特権を持つ攻撃者は、アプリケーションインターフェイス内に保存される要求の中にスクリプトまたはHTMLコンテンツを含む悪意のある入力を送信することで、こ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、攻撃者は該当アプリケーションの他のユーザに対してXSS攻撃を実行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:CSCwf81870、CSCwf83565
CVE ID：CVE-2023-20257
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

公開時点では、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 EPNM のリリース	First Fixed Release（修正された最初のリリース）
7.0 以前	修正済みリリースに移行。
7.1	7.1.1

Cisco Prime Infrastructure のリリース	First Fixed Release（修正された最初のリリース）
3.9 以前	修正済みリリースに移行。
3.10	3.10.4 Update 2

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NATO Cyber Security Center(NCSC)のJérôme Nokin氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-wkZJeyeq

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-JAN-10

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。