Cisco Evolved Programmable Network ManagerおよびCisco Prime Infrastructureに保存されている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-epnmpi-sxss-GSScPGY4
初公開日 : 2025-04-02 16:00
バージョン 1.0 : Final
CVSSスコア : 6.1
回避策 : No workarounds available
Cisco バグ ID : CSCwm66634 CSCwi92642 CSCwi89264 CSCwi89344 CSCwi37231 CSCwm66949 CSCwm51867 CSCwi55038 CSCwi95616

CVE-2025-20120
CVE-2025-20203

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Webベースの管理インターフェイス(Web GUI)における複数の脆弱性により、リモート攻撃者が該当システムのインターフェイスのユーザに対してストアドクロスサイトスクリプティング(XSS)攻撃を実行できる危険性があります。

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-epnmpi-sxss-GSScPGY4

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、次のシスコ製品に影響を与えていました。

- EPNM（必須）
- Prime インフラストラクチャ

このアドバイザリの公開時点で脆弱性が存在するシスコソフトウェア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-2025-20120:Cisco EPNMおよびCisco Prime Infrastructureのストアド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、認証されていないリモートの攻撃者が該当デバイスの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データフィールドに悪意のあるコードを挿入することにより、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: CSCwm66634、CSCwm66949
CVE ID：CVE-2025-20120
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-2025-20203:Cisco EPNMおよびCisco Prime Infrastructureのストアド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該当デバイスの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データフィールドに悪意のあるコードを挿入することにより、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。この脆弱性を不正利用するには、攻撃者は有効な管理者クレデンシャルを持っている必要があります。

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。

Bug ID(s): CSCwi37231、CSCwi55038、CSCwi89264、CSCwi89344、CSCwi92642、CSCwi95616、CSCwm51867
CVE ID：CVE-2025-20203
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完全なアップグレード ソリューション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、次の表の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た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。

CVE-2025-20120

Cisco EPNM のリリース	First Fixed Release (修正された最初のリリース)
6.1 以前	6.1.2.3
7.1	7.1.3.1
8.0	8.0.0.1
8.1	脆弱性なし

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	3.10.6.1

CVE-2025-20203

Cisco EPNM のリリース	First Fixed Release (修正された最初のリリース)
7.1 以前	修正済みリリースに移行。
8.0	8.0.0.1
8.1	脆弱性なし

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	3.10.6.1

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-2025-20120：この脆弱性を報告していただいたJakub Buczak氏に感謝いたします。

CVE-2025-20203：この脆弱性は、シスコのRoberto Petrilloによって内部セキュリティテスト中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnmpi-sxss-GSScPGY4

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	2025年4月2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。