Cisco Application Policy Infrastructure Controllerの脆弱性

Medium

アドバイザリーID : cisco-sa-apic-multi-vulns-9ummtg5
初公開日 : 2025-02-26 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 : CSCwk18862 CSCwk18863 CSCwk18864 CSCwk18865

CVE-2025-20117
CVE-2025-20118
CVE-2025-20119
CVE-2025-20116

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 Application Policy Infrastructure Controller(APIC)の複数の脆弱性により、認証された攻撃者が機密情報にアクセスしたり、任意のコマンドを実行したり、サービス妨害(DoS)状態を引き起こしたり、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。

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-apic-multi-vulns-9ummtg5

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、Cisco APICに影響を与えました。

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

脆弱性の詳細は以下のとおりです。

CVE-2025-20119:Cisco APIC認証済みローカルDoS脆弱性

Cisco APICのシステムファイル許可処理における脆弱性により、認証されたローカル攻撃者が重要なシステムファイルを上書きして、DoS状態を引き起こす可能性があります。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。

この脆弱性は、システムファイルを処理する際の競合状態に起因します。攻撃者は、ファイルシステムに対して特定の操作を実行することで、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、攻撃者がシステムファイルを上書きして、デバイスが不整合な状態になり、DoS状態が発生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: CSCwk18865
CVE ID：CVE-2025-20119
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:N/I:H/A:H

CVE-2025-20117:Cisco APIC認証済みコマンドインジェクションの脆弱性

Cisco APICのCLIの脆弱性により、認証されたローカル攻撃者が、該当デバイスの基盤となるオペレーティングシステムでルートとして任意のコマンドを実行でき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。

この脆弱性は、特定のCLIコマンドに渡される引数の検証が不十分であることに起因します。攻撃者は、巧妙に細工された入力を該当CLIコマンドの引数として含めることによって、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root権限を使用して、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: CSCwk18862
CVE ID：CVE-2025-20117
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.1
CVSSベクトル：CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:N

CVE-2025-20116:Cisco APICストアドXSSの脆弱性

Cisco APICのWeb UIの脆弱性により、認証されたリモートの攻撃者が該当システムでストアドXSS攻撃を実行でき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。

この脆弱性は、Web UIの入力検証が不適切なことに起因します。認証された攻撃者は、Web UI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Web UI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。

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: CSCwk18863
CVE ID：CVE-2025-20116
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

CVE-2025-20118:Cisco APIC認証情報漏えいの脆弱性

Cisco APICの内部システムプロセスの実装における脆弱性により、認証されたローカル攻撃者が該当デバイスの機密情報にアクセスでき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。

この脆弱性は、システムCLIコマンドで表示される機密情報のマスキングが不十分であることに起因します。攻撃者は、デバイスのCLIで偵察技術を使用することで、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、攻撃者は影響を受けるデバイスの機密情報にアクセスし、その情報を利用して攻撃を行う可能性があります。

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: CSCwk18864
CVE ID：CVE-2025-20118
SIR：中
CVSS ベーススコア：4.4

CVSSベクトル：CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/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

次の表では、左の列にシスコソフトウェアのリリースを記載しています。右側の列は、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、およびこの脆弱性に対する修正を含む最初のリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

Cisco APICリリース	First Fixed Release（修正された最初のリリース）
5.3 以前	修正済みリリースに移行。
6.0	6.0(8e)
6.1	6.1(2f)

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は、このアドバイザリに記載されている脆弱性の公表や悪用を認識していません。

出典

シスコは、これらの脆弱性を報告していただいたNATOサイバーセキュリティセンター(NCSC)のJean-Michel Huguet氏とJorge Escabias氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apic-multi-vulns-9ummtg5

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2月26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。