Cisco Application Policy Infrastructure Controllerの不正なポリシーアクションの脆弱性

Medium

アドバイザリーID : cisco-sa-apic-cousmo-uBpBYGbq
CVE-2024-20279
初公開日 : 2024-08-28 16:00
バージョン 1.0 : Final
CVSSスコア : 4.3
回避策 : No workarounds available
Cisco バグ ID : CSCwe67288

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)の制限付きセキュリティドメイン実装における脆弱性により、認証されたリモートの攻撃者が、該当システムのデフォルトのシステムポリシー(Quality of Service(QoS)ポリシーなど)の動作を変更できる可能性があります。

この脆弱性は、制限されたセキュリティドメインを使用してマルチテナントを実装する際の、不適切なアクセスコントロールに起因します。制限付きセキュリティドメインに関連付けられた有効なユーザアカウントを持つ攻撃者は、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者は、ファブリック内のすべてのテナントによって暗黙的に使用されるデフォルトのシステムポリシーの下で作成された子ポリシーを読み取り、変更、または削除し、ネットワークトラフィックを中断させる可能性があります。攻撃者がアクセスを許可されていないテナント下のポリシーでは、不正利用は不可能です。

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。

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-cousmo-uBpBYGbq

該当製品

脆弱性のある製品

公開時点で、ポート管理権限を持つ関連ユーザが制限付きセキュリティドメインに設定されて

いる場合、この脆弱性はCisco APICに影響を与えました。

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。最新情報については、本アドバイザリの冒頭に記載されているバグIDの「詳細」セクションを参照してください。

制限されたセキュリティドメイン設定とユーザポート管理アクセス許可の決定

制限付きセキュリティドメインが設定されているかどうかを確認するには、moquery -c aaaDomain -f 'aaa.Domain.restrictedRbacDomain=="yes"' | egrep dnコマンドを実行します。次に例を示します。

<#root>

apic1#

moquery -c aaaDomain -f 'aaa.Domain.restrictedRbacDomain=="yes"' | egrep dn

dn : uni/userext/domain-company1
dn : uni/userext/domain-company2

ユーザがポート管理権限を持っているかどうかを確認するには、moquery -c aaaUserRole -f 'aaa.UserRole.name=="port-mgmt"'を実行します。 | egrep dnコマンドを実行します。次に例を示します。

<#root>

apic1#

moquery -c aaaUserRole -f 'aaa.UserRole.name=="port-mgmt"' | egrep dn

dn : uni/userext/user-company1-admin/userdomain-all/role-port-mgmt
dn : uni/userext/user-company2-admin/userdomain-all/role-port-mgmt

設定がこの脆弱性の影響を受けるのは、port-mgmt権限を持つユーザが制限付きセキュリティドメインに関連付けられている場合だけです。設定がこの脆弱性の影響を受けるためには、上記の両方のクエリでエントリを返す必要があります。

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 Cloud Network Controller（旧称Cloud APIC）には影響を与えないことを確認しました。

詳細

制限付きセキュリティドメインは、テナントレベル以外のポリシーおよびプロファイルでマルチテナント機能を提供するために使用されます。これらのポリシーおよびプロファイルがどのテナントにも属していない場合でも、各テナントの個別の制限付きセキュリティドメインを使用することで、各テナントのユーザは他のテナントのユーザには見えないポリシーおよびプロファイルを作成できます。

セキュリティドメインを使用したアクセス制限の詳細については、『Cisco APICセキュリティ設定ガイド』を参照してください。

回避策

こ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。最新情報については、本アドバイザリの冒頭に記載されているバグIDの「詳細」セクションを参照してください。

左側の列にはシスコソフトウェアリリース、右側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 APIC のリリース	First Fixed Release（修正された最初のリリース）
5.2 以前	修正済みリリースに移行。
5.3	5.3(2c)
6.0	6.0(6c)
6.1	脆弱性なし

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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apic-cousmo-uBpBYGbq

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年8月28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。