Cisco Application Policy Infrastructure Controller アプリケーションの特権昇格の脆弱性

アドバイザリーID : cisco-sa-capic-chvul-CKfGYBh8
CVE-2021-1579
初公開日 : 2021-08-25 16:00
最終更新日 : 2022-06-07 17:29
バージョン 1.2 : Final
CVSSスコア : 8.1
回避策 : No workarounds available
Cisco バグ ID : CSCvw57164

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）および Cisco Cloud Application Policy Infrastructure Controller（Cloud APIC）の API エンドポイントの脆弱性により、管理者の読み取り専用クレデンシャルを持つ認証されたリモートの攻撃者が、該当システムで権限を昇格させる可能性があります。

この脆弱性は、ロールベース アクセス コントロール（RBAC）が不十分なことに起因します。管理者の読み取り専用クレデンシャルを持つ攻撃者は、管理者の書き込みクレデンシャルが設定されたアプリケーションを使用して特定の API 要求を送信することで、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、書き込み権限を持つ管理者に権限を昇格できるようになります。

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。

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-capic-chvul-CKfGYBh8

該当製品

脆弱性のある製品

この脆弱性は、Cisco APIC および Cisco Cloud APIC デバイスに管理者の書き込み権限を設定

したアプリケーションがインストールされ、有効になっている場合に影響を与えます。

管理者による書き込みが有効になっているアプリケーションがデバイスにあるかどうかを確認するには、次の手順を実行します。

1. Web UI を開き、[アプリケーション（Apps）] タブをクリックします。
2. インストールされ、有効になっているアプリケーション（[オープン（Open）] と表示されます）にマウスポインタを合わせます。右上に 4 つのアイコンが表示されます。
3. 左端のアイコンをクリックすると、アプリケーションの権限と権限レベルが表示されます。[権限：管理（Permissions:admin] と [権限レベル：書き込み（Permission Level:write）] が表示される場合、デバイスはこの脆弱性の影響を受けます。

脆弱性が存在する Cisco 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。

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。

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、管理者は、管理者の書き込み権限が有効になっているすべてのアプリケーションを無効化または削除できます。

これらのアプリケーションを無効化または削除するには、次の手順を実行します。

1. Web UI を開き、[アプリケーション（Apps）] タブをクリックします。
2. インストールされ、有効になっているアプリケーション（[オープン（Open）] と表示されます）にマウスポインタを合わせます。右上に 4 つのアイコンが表示されます。
3. アプリケーションを無効にするには、線が入った円のアイコンをクリックします。アプリケーションを削除するには、[X] アイコンをクリックします。

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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのよ

うなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

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ているかどうか、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 または Cisco Cloud APIC ソフトウェアリリース	First Fixed Release（修正された最初のリリース）
3.2 より前	修正済みリリースに移行。
3.2	3.2(10f)
4.0	修正済みリリースに移行。

Cisco APIC または Cisco Cloud APIC ソフトウェアリリース	First Fixed Release（修正された最初のリリース）
4.1	修正済みリリースに移行。
4.2	4.2(7l)
5.0	修正済みリリースに移行。
5.1	修正済みリリースに移行。
5.2	5.2(2f)

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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を確認していません。

出典

この脆弱性は、Cisco Advanced Security Initiatives Group（ASIG）の Arthur Vidineyev による内部セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-chvul-CKfGYBh8

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.2	元のCVSSスコアに戻しました。	Header	Final	2022 年 6 月 7 日
1.1	脆弱性ソースを更新。	出典	Final	2022 年 3 月 8 日
1.0	初回公開リリース	—	Final	2021 年 8 月 25 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。