Cisco Application Policy Infrastructure Controllerのコマンドインジェクションとファイルアップロードの脆弱性

Medium

アドバイザリーID : cisco-sa-capic-mdvul-HBsJBuvW
初公開日 : 2021-08-25 16:00
最終更新日 : 2022-03-08 16:52
バージョン 1.1 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCvw57577 CSCvw57581

CVE-2021-1580
CVE-2021-1581

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)またはCisco Cloud APICのWeb UIおよびAPIエンドポイント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に対してコマンドインジェクションまたはファイルアップロード攻撃を実行する可能性があります。

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-capic-mdvul-HBsJBuvW

該当製品

脆弱性のある製品

公開時点では、これらの脆弱性はCisco APICおよびCloud APICに影響を与えていました。

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。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-2021-1580:Cisco APICのコマンドインジェクションの脆弱性

Cisco APICのWeb UIまたはCisco Cloud APICのAPIエンドポイントの脆弱性により、認証されたリモート攻撃者が該当デバイスに対してコマンド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、Web UIおよびAPIエンドポイントでの入力の検証が不適切なことに起因します。高い権限を持つ攻撃者は、特定のコマンドの実行中に巧妙に細工された入力を挿入することで、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、攻撃者は該当デバイスでrootレベルの権限を使用して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:CSCvw57577
CVE ID：CVE-2021-1580
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

CVE-2021-1581:Cisco APICのファイルアップロードの脆弱性

Cisco APICまたはCisco Cloud APICのAPIエンドポイントの脆弱性により、認証されていないリモートの攻撃者が該当デバイスにファイルをアップロードできる可能性があります。

この脆弱性は、不適切なアクセス制御に起因します。攻撃者は、特定のAPIエンドポイントを使用して該当デバイスにファイルをアップロードすることにより、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、攻撃者は該当デバイスのアップロードパーティションがいっぱいにな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:CSCvw57581
CVE ID：CVE-2021-1581
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:N/UI:N/S:U/C:N/I:L/A:L

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

発行時点では、次の表に記載されている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。

左の列はシスコソフトウェアリリースを示し、右の列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を示します。

APICコマンドインジェクションの脆弱性：CSCvw57577

Cisco APICおよびクラウドAPICリリース	この脆弱性に対する最初の修正リリース
3.2 より前	修正済みリリースに移行。
3.2	3.2(10e)
4.0	修正済みリリースに移行。
4.1	修正済みリリースに移行。
4.2	4.2(6h)
5.0	修正済みリリースに移行。

Cisco APICおよびクラウドAPICリリース	この脆弱性に対する最初の修正リリース
5.1	5.1(3e)
5.2	5.2(1g)

APICファイルアップロードの脆弱性：CSCvw57581

Cisco APICおよびクラウドAPICリリース	この脆弱性に対する最初の修正リリース
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。
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(1g)

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例とその公表は確認しておりません。

出典

これらの脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のArthur Vidineyevによる社内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-mdvul-HBsJBuvW

改訂履歴

バージョン	説明	セクション	ステータス	日付
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

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものでは

ありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。