

Cisco AppDynamics Controllerのクロスサイトスクリプティングの脆弱性



アドバイザリーID : cisco-sa-appd-xss-

3JwqSMNT

初公開日 : 2024-03-06 16:00

バージョン 1.0 : Final

CVSSスコア : [5.4](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwh29203](#)

[CVE-2024-](#)

[20346](#)

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 AppDynamics ControllerのWebベース管理インターフェイスにおける脆弱性により、認証されたりモートの攻撃者が、該当デバイスのインターフェイスのユーザに対して反映クロスサイトスクリプティング(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によるユーザ入力の検証が不十分であることに起因します。攻撃者は、悪意のあるリンクをクリックするようにユーザを誘導することで、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。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-xss-3JwqSMNT>

該当製品

脆弱性のある製品

この脆弱性は、クラウドベースのCisco AppDynamics Controllerに影響を与えます。

公開時点では、この脆弱性はAppDynamics Controller On-Premiseにも影響を与えました。

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。

修正済みソフトウェア

シスコのAppDynamicsは、このアドバイザリに記載された脆弱性に対処するためのソフトウェアアップデートをリリースしました。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、最新のライセンスを保持し、有効なサポートとメンテナンス契約を持つソフトウェアバージョンとフィーチャセットのみです。こ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するにより、お客様はAppDynamicsとのライセンス契約の条項に従うことに同意したことになります。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や追加のソフトウェア フィーチャ セットに対する権限が付与されることはありません。

有効なサポートとメンテナンスの契約を持ち、現在のライセンスをお持ちのお客様は、既存のAppDynamics配信サーバーのダウンロードアカウントから修正済みバージョンのソフトウェアをダウンロードできます。

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。情報が不明な場合は、AppDynamics Supportシステムでサポートチケットを開くことをお勧めします。

修正済みリリース

AppDynamicsは、クラウドベースのSoftware as a Service(SaaS)環境でこの脆弱性に対処しています。SaaSバージョンのCisco AppDynamics Controllerをご使用のお客様は、ユーザ操作は必要ありません。

AppDynamics Controllerオンプレミス

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Cisco AppDynamics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を示しています。

Cisco AppDynamics Controllerリリース	First Fixed Release (修正された最初のリリース)
23.4.0 より前	23.4.0

修正済みリリースは、AppDynamicsソフトウェアポータル(<https://download.appdynamics.com>)から入手できます。修正済みソフトウェアをダウンロードするには、お客様にAppDynamicsアカウントが必要です。

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-appd-xss-3JwqSMNT>

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3月6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、単独の転載や意識を施した場合、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。