Cisco AppDynamics PHPエージェントの権限昇格の脆弱性

Medium

アドバイザリーID : cisco-sa-appd-php-authpriv-gEBwTvu5

CVE-2023-20274

初公開日 : 2023-11-15 16:00

バージョン 1.0 : Final

CVSSスコア : 6.3

回避策 : No workarounds available

Cisco バグ ID : CSCwh65119

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 PHP Agentのインストーラスクリプトの脆弱性により、認証されたローカル攻撃者が該当デバイスの権限を昇格できる可能性があります。

この脆弱性は、PHPエージェントインストーラによってPHPエージェントのインストールディレクトリに設定される権限が不十分であることに起因します。攻撃者は、PHPと同じ権限で実行されるPHPエージェントのインストールディレクトリ内のオブジェクトを変更することで、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、権限の低い攻撃者は該当デバイスで権限をルートに昇格できるようになります。

Cisco AppDynamics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-appd-php-authpriv-gEBwTvu5

該当製品

脆弱性のある製品

この脆弱性は、公開時点でCisco AppDynamics PHP Agent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

シスコの会社であるAppDynamicsは、このアドバイザリに記載されている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ことにより、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締結し、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

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 PHP Agentリリース	First Fixed Release（修正された最初のリリース）
23.4.0 以前	23.7.0

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、AppDynamicsアカウントが必

要です。

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

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-php-authpriv-gEBwTvu5

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	2023-NOV-15

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。