Cisco Meraki Systems Manager Agent for Windowsの権限昇格の脆弱性

アドバイザリーID : cisco-sa-meraki-agent-dll-hj-Ptn7PtKe
CVE-2024-20430
初公開日 : 2024-09-04 16:00
バージョン 1.0 : Final
CVSSスコア : 7.3
回避策 : No workarounds available
Cisco バグ ID :

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 Meraki Systems Manager(SM)Agent for Windowsの脆弱性により、認証されたローカルの攻撃者が特権権限を使用して任意のコードを実行する可能性があります。

この脆弱性は、実行時のディレクトリ検索パスの不適切な処理に起因します。権限の低い攻撃者は、該当システムに悪意のあるコンフィギュレーションファイルと悪意のあるDLLファイルの両方を配置することで、この脆弱性をエクスプロイトし、Cisco Meraki SMが起動時にファイルを読み取って実行する可能性があります。エクスプロイトに成功すると、攻撃者はシステム権限を使用して該当システム上で任意のコードを実行できる可能性があります。

Cisco Meraki では、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-meraki-agent-dll-hj-Ptn7PtKe

該当製品

脆弱性のある製品

この脆弱性は、 Cisco Meraki SM Agent for Windowsです。

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。

シスコでは、この脆弱性が Cisco Meraki SM Agent for Macです。

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

Cisco Meraki では、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リリースとフィーチャセットに対してのみとなります。お客様は、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、シスコ エンド ユーザー ライセンス契約および該当する製品固有の条件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、Cisco Meraki から直接、あるいは Cisco Meraki 認定リセラーやパートナーから、ソフトウェアの有効なライセンスを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。

お客様は、[Cisco Security Advisories] ページで入手できる Cisco Meraki 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完全なアップグレード ソリューションを確認することをお勧めします。

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。Cisco Meraki は、ファームウェアの更新にファームウェアのベストプラクティスを利用することを推奨しています。情報が明確でない場合は、Cisco Meraki サポートに問い合わせることをお勧めします。

修正済みリリース

Cisco Merakiは、2024年6月12日にMerakiダッシュボードを通じて、この脆弱性に対する修正を含むアップデートをリリースしました。Cisco Merakiは、Cisco Meraki SM Agent for Windowsリ

リース4.2.0以降に直ちにアップグレードすることを推奨します。Cisco Meraki Systems Manager Agentリリース4.2.0のリリースノートは、https://documentation.meraki.com/SM/Device_Enrollment/Systems_Manager_Agent_Release_Notesで確認できます。

Merakiダッシュボードのエージェントバージョン管理が最新またはリリース4.2.0以降に設定されているシステムでは、エージェントの導入は自動的に修正済みリリースにアップグレードされます。ネットワーク上の複数のデバイスまたは特定のデバイスにエージェントバージョンを設定する方法については、「システムマネージャエージェントとMDMプロファイルの登録」を参照してください。

不正利用事例と公式発表

本アドバイザリの公開時点で、Cisco Meraki 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不正利用事例とその公表は確認しておりません。

出典

Cisco Merakiは、Cisco Meraki Bugcrowdプログラムを通じてこの脆弱性を報告していただいたBugcrowdユーザJony_Juiceに感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-agent-dll-hj-Ptn7PtKe

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9月4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。