

Cisco Secure Endpoint for Windows スキャン回避の脆弱性



アドバイザリーID : cisco-sa-secure-endpoint-dos-RzOgFKnd

[CVE-2023-20084](#)

初公開日 : 2023-11-15 16:00

バージョン 1.0 : Final

CVSSスコア : [5.0](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwh78740](#)

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 Secure Endpoint for Windowsのエンドポイントソフトウェアの脆弱性により、認証されたローカルの攻撃者が、制限時間内にエンドポイントの保護を回避できる可能性があります。

この脆弱性は、さまざまなソフトウェアコンポーネント間で発生するタイミングの問題に起因します。攻撃者は、悪意のあるファイルを特定のフォルダに配置するようにユーザを誘導し、制限時間内にファイルを実行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、攻撃者はエンドポイントソフトウェアで悪意のあるファイルの検疫に失敗させたり、プロセスを強制終了させたりする可能性があります。

注：この脆弱性は、Windowsフォルダリダイレクション機能が有効になっている展開にのみ適用されます。

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-secure-endpoint-dos-RzOgFKnd>

該当製品

脆弱性のある製品

公開時点では、この脆弱性はCisco Secure Endpoint Connector for WindowsおよびCisco Secure Endpoint Private Cloud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。](#)

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- Linux 向け Cisco Secure Endpoint Connector
- MacOS 向け Cisco Secure Endpoint Connector

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

[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。

シスコ プラットフォーム	First Fixed Release (修正された最初のリリース)
Windows 向け Cisco Secure Endpoint Connector	7.5.17 (Nov 2023) 8.2.1.21650
セキュアエンドポイントプライベートクラウド	4.1

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りリ

—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

この脆弱性はシスコのKevin Scheel氏によって発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-endpoint-dos-RzOgFKnd>

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。