Cisco AnyConnectセキュアモビリティクライアントを使用したMacOSのローカル権限昇格

アドバイザリーID : cisco-sa-anyconnect-mac-priv-esc-VqST2nrT
初公開日 : 2021-05-05 16:00
最終更新日 : 2021-05-11 13:40
バージョン 1.1 : Final
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

2020年5月26日、AppleはMacOS Catalina、Mojave、およびHigh Sierraのセキュリティアップデートをリリースしました。このアップデートの一部では、ローカルの権限昇格の脆弱性(CVE-2020-9817)に対処しています。

シスコは、Cisco AnyConnectセキュアモビリティクライアントリリース4.10.00093以前を使用してこの脆弱性を不正利用する可能性があると判断しています。

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-anyconnect-mac-priv-esc-VqST2nrT

詳細

MacOSインストーラプロセスは、実行前にアプリケーションパッケージの内容を一時フォルダに抽出します。これらのファイルの所有権をrootユーザに割り当てる代わりに、開発者のシステムからの元のUIDが維持されます。抽出されたファイルと同じUIDを持つローカル攻撃者は、root権限を使用して基盤となるオペレーティングシステム上でコードを実行するようにファイルを変更する可能性があります。

この脆弱性の詳細については、次のリンクを参照してください。

- macOS Catalina 10.15.5、Security Update 2020-003 Mojave、Security Update 2020-003 High Sierraのセキュリティコンテンツについて
- テクニカルアドバイザリ – macOS Installer Local Root Privilege Escalation(CVE-2020-9817)

シスコでは、Cisco Bug ID CSCvw22016でこの問題を追跡しています。

推奨事項

シスコのアプリケーションまたは製品が稼働している、該当するすべてのオペレーティングシステムにAppleセキュリティアップデートを適用することをお勧めします。

シスコは、次のリリースでCisco AnyConnectセキュアモビリティクライアントを更新し、このMacOSインストーラの脆弱性に対処する予定です。

出典

シスコは、この脆弱性を報告していただいたLockheed Martin Red Teamに感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-mac-priv-esc-VqST2nrT

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	Cisco Bug IDへの参照を追加。	詳細	Final	2021年5月11日
1.0	初回公開リリース	—	Final	2021 年 5 月 5 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。