

フレーミングフレーム：複数のシスコ製品に影響を与える送信キューの操作によるWi-Fi暗号化のバイパス



Advisory ID : cisco-sa-wifi-ffeb-22epcEWu

初公開日 : 2023-03-27 05:00

バージョン 1.0 : Final

回避策 : No workarounds available

Cisco Bug ID :

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

概要

2023年3月27日に、調査報告書『フレームのフレーミング：送信キューの操作によるWi-Fi暗号化のバイパス』が公開されました。このドキュメントでは、802.11標準の脆弱性について説明します。この脆弱性により、攻撃者はターゲットのワイヤレスクライアントをスプーフィングして、アクセスポイントの送信キュー内にあるフレームを攻撃者によって制御されるデバイスにリダイレクトできるようになります。この攻撃は日和見攻撃と見なされ、攻撃者によって得られる情報は、安全に設定されたネットワークでは最小限の価値しかありません。

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-wifi-ffeb-22epcEWu>

該当製品

ホワイトペーパーで概説されている攻撃は、Cisco Wireless Access Point(WAP)製品およびワイヤレス機能を備えたCisco Meraki製品に対して利用することで成功する可能性があります。

推奨事項

本書で概説されている攻撃が成功する可能性を減らすために、シスコでは、Cisco Identity Services Engine(ISE)などのシステムを通じてポリシー適用メカニズムを使用することを推奨しています。ISEでは、Cisco TrustSecまたはSoftware Defined Access(SDA)テクノロジーを実装してネットワークアクセスを制限できます。また、取得したデータが攻撃者によって使用できなくなる可能性があるため、トランスポート層セキュリティを実装して、伝送中のデータを可能な限り暗号化することをお勧めします。

不正利用事例と公式発表

Cisco Product Security Incident Response Team(PSIRT)は、このアドバイザリに記載された脆弱性に対して概念実証用の 익스プロイトコードが入手可能であることを認識しています。これは、次のGitHubリポジトリで研究者が利用できるようになりました
: <https://github.com/vanhoefm/macstealer>

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は確認しておりません。

出典

これらの脆弱性は、ニューヨーク大学アブダビ校のMathy Vanhoef博士によってシスコに報告されたものです。シスコは、これらの脆弱性に対処する際の継続的な支援とサポートに対してVanhoef博士に感謝します。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wifi-ffeb-22epcEWu>

改訂履歴

バージョン	説明	セクション	Status	日付
1.0	初版リリース	—	Final	2023年3月27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ー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。