# RADIUS プロトコルスプーフィングの脆弱性（Blast-RADIUS）：2024 年 7 月


アドバイザリーID : cisco-sa-radius-spoofing-july-2024-87cCDwZ3
初公開日 : 2024-07-10 16:00
最終更新日 : 2024-08-09 19:53
バージョン 1.8 : Final
CVSSスコア : 8.1
回避策 : No workarounds available
Cisco バグ ID :

CVE-2024-3596

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

2024 年 7 月 7 日、セキュリティ研究者が、RADIUS プロトコルの次の脆弱性を公開しました。

CVE-2024-3596：RFC 2865 に基づく RADIUS プロトコルは、オンパス攻撃者によるフォージェリ攻撃の影響を受ける可能性があります。この攻撃では、攻撃者が、MD5 応答オーセンティケータ署名に対する選択プレフィックス衝突攻撃を使用して、有効な応答（Access-Accept、Access-Reject、または Access-Challenge）を別の応答に変更できます。

この脆弱性は、すべての RADIUS クライアントおよびサーバーに影響を与える可能性があります。この脆弱性の説明については、『RADIUS protocol susceptible to forgery attacks.』（VU#456537）を参照してください。

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-radius-spoofing-july-2024-87cCDwZ3

## 該当製品

シスコでは、この脆弱性の影響を受ける製品およびクラウドサービスを判断するために、製品ラインを調査しました。

「脆弱性のある製品」のセクションで、影響を受ける各製品またはサービスの Cisco Bug ID を示します。Cisco Bug は Cisco Bug Search Tool で検索可能であり、回避策（使用可能な場合）と修正されたソフトウェア リリースなど、プラットフォーム固有の追加情報が記載されます。

## 脆弱性のある製品

次の表に、本アドバイザリに記載された脆弱性の影響を受けるシスコ製品を示します。詳細については、関連するシスコのバグを参照してください。

| 製品 | Cisco Bug ID |
|---|---|
| エンドポイント クライアントとクライアント ソフトウェア | |
| Duo Authentication Proxy | CSCwk87884 |
| ネットワークおよびコンテンツ セキュリティ デバイス | |
| 適応型セキュリティ アプライアンス（ASA） | CSCwk71992 |
| Firepower Device Manager（FDM） | CSCwk69454 |
| Firepower Management Center（FMC）ソフトウェア | CSCwk71817 |
| Firepower Threat Defense（FTD）ソフトウェア | CSCwk67902 |
| Meraki MX シリーズ | 注意事項 |
| Identity Services Engine（ISE） | CSCwk67747 |
| Secure Email Gateway | CSCwk70832 |
| Cisco Secure Email and Web Manager | CSCwk70833 |
| Secure Firewall | CSCwk67859 |
| Cisco Secure Network Analytics | CSCwk73619 |
| Cisco Secure Web Appliance | CSCwk70834 |
| ネットワーク管理とプロビジョニング | |
| Application Policy Infrastructure Controller（APIC） | CSCwk70836 |
| Crosswork Network Controller | CSCwk70850 |
| Nexus Dashboard,（旧称：Application Services Engine） | CSCwk70840 |
| Prime インフラストラクチャ | CSCwk79727 |
| Routing and Switching - Enterprise and Service Provider | |
| ASR 5000 シリーズ ルータ | CSCwk70831 |
| Catalyst Center | CSCwk70845 |
| Catalyst SD-WAN コントローラ（旧称、SD-WAN vSmart） | CSCwk70854 |
| Catalyst SD-WAN Manager（旧称、SD-WAN vManage） | CSCwk70854 |
| Catalyst SD-WAN Validator（旧称、SD-WAN vBond） | CSCwk70854 |
| GGSN Gateway GPRS Support Node | CSCwk70831 |
| IOS ソフトウェア | CSCwk78278 |
| IOS XE ソフトウェア | CSCwk70852 |

| | |
|---|---|
| IOS XR ソフトウェア | CSCwk70236 |
| IOx Fog Director | CSCwk70851 |
| MDS 9000 シリーズ マルチレイヤ スイッチ | CSCwk70837 |
| Nexus 1000V シリーズ スイッチ | CSCwk79691 |
| Nexus 3000 シリーズ スイッチ | CSCwk70839 |
| Nexus 5500 プラットフォーム スイッチ | CSCwk79692 |
| Nexus 5600 プラットフォーム スイッチ | CSCwk79692 |
| Nexus 6000 シリーズ スイッチ | CSCwk79692 |
| Nexus 7000 シリーズ スイッチ | CSCwk70838 |
| ACI モードの Nexus 9000 シリーズ ファブリック スイッチ | CSCwk83051 |
| スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ | CSCwk70839 |
| PGW Packet Data Network Gateway | CSCwk70831 |
| SD-WAN vEdge ルータ | CSCwk70854 |
| System Architecture Evolution（SAE）ゲートウェイ | CSCwk70831 |
| Ultra Packet Core | CSCwk70831 |
| Unified Computing | |
| エンタープライズ NFV インフラストラクチャ ソフトウェア（NFVIS） | CSCwk79647 |
| UCS Central Software | CSCwk71967 |
| UCS マネージャ | CSCwk70842 |
| ワイヤレス ユニファイド コンピューティング | |
| AireOS ワイヤレス LAN コントローラ | CSCwk70846 |

## 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。

ネットワーク アプリケーション、サービス、およびアクセラレーション

- Nexus Dashboard Insights（オンプレミス）
- Cisco Secure Workload

ネットワークおよびコンテンツ セキュリティ デバイス

- Firepower 4100/9300 FXOS Firepower Chassis Manager

- Cisco Secure Malware Analytics アプライアンス
- Cisco Umbrella Active Directory（AD）コネクタ

ネットワーク管理とプロビジョニング

- Cisco Evolved Programmable Network Manager（EPNM）
- Cisco DNA Spaces コネクタ
- Policy Suite

Routing and Switching - Enterprise and Service Provider

- Ultra Cloud Core：ポリシー制御機能

Unified Computing

- UCS B シリーズ ブレード サーバ

ワイヤレス

- 6300 シリーズ エンベデッド サービス アクセス ポイント
- Aironet 1540 シリーズ
- Aironet 1560 シリーズ
- Aironet 1810 シリーズ OfficeExtend アクセスポイント
- Aironet 1810w シリーズ アクセス ポイント
- Aironet 1815 シリーズ アクセス ポイント
- Aironet 1830 シリーズ アクセス ポイント
- Aironet 1850 シリーズ アクセス ポイント
- Aironet 2800 シリーズ アクセス ポイント
- Aironet 3800 シリーズ アクセス ポイント
- Aironet 4800 アクセスポイント
- Aironet 802.11ac Wave 2 アクセスポイント
- Catalyst 9100 シリーズ アクセスポイント
- Catalyst IW6300 Heavy Duty シリーズ アクセスポイント
- Catalyst IW9165 Heavy Duty シリーズ
- Catalyst IW9165 高耐久性シリーズ
- Catalyst IW9167 Heavy Duty シリーズ

## 回避策

この脆弱性に対処する回避策はありません。

DTLS over TCP または TLS over TCP を使用するように設定された RADIUS クライアントおよびサーバーは、トラフィックがプレーンテキストで送信されない限り、基盤となる実装にその他の点で脆弱性があってもエクスプロイトされません。

お客様は、ご使用の環境および使用条件において、この緩和策の適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

## 修正済みソフトウェア

修正済みソフトウェアリリースの詳細については、本アドバイザリの「脆弱性のある製品」セクションに記載されている Cisco Bug ID を参照してください。

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。

## 不正利用事例と公式発表

Cisco PSIRT は、このアドバイザリで説明されている脆弱性に対してコンセプト実証エクスプロイトコードが利用可能であることを認識しています。

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

## 出典

この脆弱性は、2024 年 7 月 9 日に、Sharon Goldberg 氏、Miro Haller 氏、Nadia Heninger 氏、Mike Milano 氏、Dan Shumow 氏、Marc Stevens 氏、および Adam Suhl 氏によって公開されました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3

## 改訂履歴

| バージョン | 説明 | セクション | ステータス | 日付 |
|---|---|---|---|---|
| 1.8 | 脆弱性があると判断された製品のリスト、および脆弱性がないと判断された製品のリストを更新。 | 「脆弱性のある製品」および「脆弱性を含んでいないことが確認された製品」 | Final | 2024 年 8 月 9 日 |
| 1.7 | 概要、現在調査中の製品のリスト、および影響を受けると判断された製品のリストを更新。 | 要約, 該当製品, 脆弱性が存在する製品, 脆弱性が存在しないことが確認された製品 | Final | 2024 年 8 月 2 日 |
| 1.6 | 現在調査中の製品のリスト、および影響を受けると判断された製品のリストを更新。 | 該当製品および脆弱性のある製品 | Interim | 2024 年 7 月 29 日 |
| 1.5 | 現在調査中の製品、影響を受けると判断された製品、および脆弱性がないと判断された製品のリストを更新。 | 該当製品, 脆弱性が存在する製品, 脆弱性を含んでいないことが確認された製品. | Interim | 2024 年 7 月 24 日 |
| 1.4 | 現在調査中の製品、影響を受けると判断された製品、および脆弱性がないと判断された製品のリストを更新。 | 該当製品, 脆弱性が存在する製品, 脆弱性を含んでいないことが確認された製品. | Interim | 2024 年 7 月 19 日 |
| 1.3 | 現在調査中の製品、影響を受けると判断された製品、および脆弱性がないと判断された製品のリストを更新。 | 該当製品, 脆弱性が存在する製品, 脆弱性を含んでいないことが確認された製品. | Interim | 2024 年 7 月 17 日 |
| 1.2 | 現在調査中の製品、影響を受けると判断された製品、および脆弱性がないと判断された製品のリストを更新。 | 該当製品, 脆弱性が存在する製品, 脆弱性を含んでいないことが確認された製品 | Interim | 2024 年 7 月 16 日 |
| 1.1 | 現在調査中の製品のリストを更新。 | 該当製品 | Interim | 2024 年 7 月 11 日 |
| 1.0 | 初回公開リリース | — | Interim | 2024 年 7 月 10 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。