Cisco Secure Clientキャリッジリターンラインフィードインジェクションの脆弱性

High

アドバイザリーID : cisco-sa-secure-client-crlf-W43V4G7
CVE-2024-20337
初公開日 : 2024-03-06 16:00
バージョン 1.0 : Final
CVSSスコア : 8.2
回避策 : No workarounds available
Cisco バグ ID : CSCwi37512

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 ClientのSAML認証プロセスの脆弱性により、認証されていないリモートの攻撃者がユーザに対してキャリッジリターンラインフィード(CRLF)インジェクション攻撃を実行する可能性があります。

この脆弱性は、ユーザ指定の入力の検証が不十分であることに起因します。攻撃者は、VPNセッションの確立中に、巧妙に細工されたリンクをクリック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、攻撃者はブラウザで任意のスクリプトコードを実行したり、有効なSAMLトークンを含むブラウザベースの機密情報にアクセスしたりする可能性があります。攻撃者はこのトークンを使用して、該当ユーザの権限でリモートアクセスVPNセッションを確立できます。VPNヘッドエンドの背後にある個々のホストとサービスは、引き続きアクセスを成功させるために追加のクレデンシャルを必要とします。

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-client-crlf-W43V4G7

該当製品

脆弱性のある製品

この脆弱性は、Cisco Secure Clientの脆弱性が存在するリリースを実行し、SAML外部ブラウ

ザ機能を使用してVPNヘッドエンドが設定されている次のシスコ製品に影響を与えます。

- Secure Client for Linux（ベータ版）
- MacOS用のセキュアクライアント
- Secure Client for Windowsの場合

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。

VPNヘッドエンド設定の確認

VPNヘッドエンドがSAML外部ブラウザ機能を使用するように設定されているかどうかを確認するには、Cisco適応型セキュリティアプライアンス(ASA)ソフトウェアまたはCisco Firepower Threat Defense(FTD)ソフトウェアのCLIでshow running-config tunnel-group特権EXECコマンドを使用します。

次に、SAML外部ブラウザ機能が有効になっているデバイスでのコマンドの出力例を示します。

```
<#root>

ciscoasa#

show running-config tunnel-group


tunnel-group EXAMPLE_GROUP type remote-access
tunnel-group EXAMPLE_GROUP webvpn-attributes
 authentication saml


saml external-browser


 saml identity-provider EXAMPLE
```

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。

- Android向けセキュアクライアントAnyConnect
- ユニバーサルWindowsプラットフォーム用のセキュアクライアント（AnyConnectを含む）

- iOS用のセキュアクライアントAnyConnect VPN

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

シスコ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。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

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 バージョンとフィーチャ セットに対してのみとなります。そ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した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項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、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから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。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連

絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。右側の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含む最初のリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

Cisco Secure Clientリリース	First Fixed Release（修正された最初のリリース）
4.10.04065 より前	脆弱性なし
4.10.04065 以降	4.10.08025
5.0	修正済みリリースに移行。
5.1	5.1.2.42

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リリー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

この脆弱性を報告していただいたAmazon SecurityのPaulos Yibero Mesfin氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-client-crlf-W43V4G7

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3月6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。