Cisco 適応型セキュリティ アプライアンス ソフトウェアのクライアントレス SSL VPN におけるヒープオーバーフローの脆弱性

High

アドバイザリーID : cisco-sa-asa-ssl-vpn-heap-zLX3FdX
CVE-2022-20737
初公開日 : 2022-04-27 16:00
最終更新日 : 2022-06-01 16:25
バージョン 1.1 : Final
CVSSスコア : 7.1
回避策 : No workarounds available
Cisco バグ ID : CSCwa33898

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 適応型セキュリティアプライアンス (ASA) ソフトウェアのクライアントレス SSL VPN ポータルを介してアクセスされるリソースの HTTP 認証ハンドラにおける脆弱性により、認証されたリモート攻撃者が、該当デバイスでサービス妨害 (DoS) 状態を発生させたり、該当デバイスからプロセスメモリの一部を取得する可能性があります。

この脆弱性は、特定の HTTP 認証メッセージを解析する際の不十分な境界チェックに起因します。攻撃者は、VPN ゲートウェイとして動作する該当デバイスに悪意のあるトラフィックを送信することにより、この脆弱性をエクスプロイトする可能性があります。この悪意のあるトラフィックを送信するには、攻撃者は、クライアントレス SSL VPN ポータルを介してアクセスできる Web サーバーを制御する必要があります。エクスプロイトに成功すると、攻撃者は、 デバイスをリロードして DoS 状態を引き起こしたり、デバイスの機密情報を含む可能性のあるプロセスメモリからバイトを取得する可能性があります。

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-asa-ssl-vpn-heap-zLX3FdX

このアドバイザリは、2022 年 4 月に公開された Cisco ASA、FTD、および FMC のセキュリティ

アドバイザリ バンドルに含まれています。アドバイザリとリンクの一覧については、Cisco Event Response：2022 年 4 月に公開された Cisco ASA、FMC、および FTD ソフトウェア セキュリティ アドバイザリ バンドル を参照してください。

該当製品

脆弱性のある製品

この脆弱性の影響を受けるのは、シスコ製品で、脆弱性のある Cisco ASA ソフトウェアリリースが実行されており、クライアントレス SSL VPN が設定されている場合です。

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。

クライアントレス SSL VPN が設定されているかどうかの確認

デバイスでクライアントレス SSL VPN が有効になっているかどうかを確認するには、次の両方を実行します。

- show running-config webvpn コマンドを使用して、少なくとも 1 つのインターフェイスに関して enable コマンドが存在することを確認します。次の例は、外部インターフェイスで SSL VPN が有効になっているデバイスのコマンド出力を示しています。

```
<#root>

cisco#

show running-config webvpn

webvpn
.
.
.

enable

 outside
.
.
.
```

- show running-config all group-policy コマンドを使用して、vpn-tunnel-protocol パラメータに ssl-clientless 値が存在することを確認します。次の例は、クライアントレス SSL VPN が有効になっているデバイスのコマンド出力を示しています。

```
<#root>

cisco#

show running-config all group-policy | include ssl-clientless
```

```
vpn-tunnel-protocol ssl-client
ssl-clientless
```

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。

- Firepower Management Center（FMC）ソフトウェア
- Firepower Threat Defense（FTD）ソフトウェア

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 Cisco Support and Downloads 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のリリースを記載しています。中央の列は、リリースがこのアドバイザリに記載されている脆弱性に該当するかどうか、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。右側の列は、リリースがこのバンドルに記載された「重大」または「高」SIR 脆弱性のいずれかに該当するかどうか、およびそれらの脆弱性に対する修正を含むリリースを示しています。

Cisco ASA ソフトウェア

Cisco ASA ソフトウェア リリース	この脆弱性に対する最初の修正リリース	アドバイザリのバンドルに記載されているすべての脆弱性に対する最初の修正済みリリース
9.7 以前[1]	修正済みリリースに移行。	修正済みリリースに移行。
9.8	9.8.4.44 (June 2022)	9.8.4.44 (June 2022)
9.91	修正済みリリースに移行。	修正済みリリースに移行。
9.101	修正済みリリースに移行。	修正済みリリースに移行。
9.12	9.12.4.38	9.12.4.38
9.131	修正済みリリースに移行。	修正済みリリースに移行。
9.14	9.14.4	9.14.4
9.15	9.15.1.21	9.15.1.21

Cisco ASA ソフトウェア リリース	この脆弱性に対する最初の修正リリース	アドバイザリのバンドルに記載されているすべての脆弱性に対する最初の修正済みリリース
9.16	9.16.2.14	9.16.2.14
9.17	9.17.1.7	9.17.1.7

1. Cisco ASA ソフトウェアリリース 9.7 以前、および 9.9、9.10、9.13 リリースについては、 ソフトウェアのメンテナンスが終了しています。この脆弱性の修正を含むサポート対象リリースに移行することをお勧めします。

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 Positive Technologies 社の Nikita Abramov 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssl-vpn-heap-zLX3FdX

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	ASA 9.8 の最初の修正済みリリースに関する情報を更新。	修正済みソフトウェア	Final	2022 年 6 月 1 日
1.0	初回公開リリース	—	Final	2022 年 4 月 27 日

利用規約

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。