Cisco 適応型セキュリティ アプライアンス ソフトウェアの SSL/TLS におけるサービス妨害の脆弱性

アドバイザリーID : cisco-sa-asa-ssl-dos-7uZWwSEy
CVE-2020-27124
初公開日 : 2020-10-22 16:00
最終更新日 : 2020-10-27 20:31
バージョン 1.1 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCvt64822

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 SSL/TLS ハンドラの脆弱性により、認証されていないリモートの攻撃者が該当デバイスの予期しないリロードを引き起こし、サービス妨害 (DoS) 状態が発生する可能性があります。

この脆弱性は、確立された SSL/TLS 接続における不適切なエラー処理に起因します。攻撃者は、該当デバイスとの SSL/TLS 接続を確立し、その接続内で悪意のある SSL/TLS メッセージ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。エクスプロイトに成功すると、攻撃者は標的デバイスのリロードを引き起こすことができるようになります。

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-dos-7uZWwSEy

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、SSL/TLS メッセージ処理を伴う機能がデバイスで有効になっている Cisco ASA ソフトウェアリリース 9.13.1.12、9.13.1.13、9.14.1.10 です。これらの機

能には次のようなものがあります。

- AnyConnect SSL VPN[1]
- クライアントレス SSL VPN[1]
- 管理インターフェイスに使用される HTTP サーバ

1. Cisco適応型セキュリティ仮想アプライアンス(ASAv)には、これらの設定に対する脆弱性はありません。

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。

デバイスで SSL または TLS メッセージ処理の可能性があるかどうかの確認

Cisco ASA ソフトウェアを実行しているデバイスで、SSL または TLS パケット処理の可能性があるかどうかを確認するには、show asp table socket コマンドを使用します。 | include SSL|DTLSコマンドを使用して、出力が返されることを確認します。このコマンドで何らかの出力が返される場合、そのデバイスには脆弱性があります。このコマンドを実行して空の結果が返される場合、そのデバイスは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ません。以下は、show asp table socket コマンドの出力例です。 | include SSL|DTLSコマンドを実行するデバイスにアクセスできない場合の出力例を示します。

```
<#root>

ftd#

show asp table socket | include SSL|DTLS


SSL        0005aa68  LISTEN     x.x.x.x:443      0.0.0.0:*
SSL        002d9e38  LISTEN     x.x.x.x:8443     0.0.0.0:*
DTLS       0018f7a8  LISTEN     10.0.0.250:443   0.0.0.0:*
```

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 Cisco Firepower Management Center（FMC）ソフトウェアまたは Cisco Firepower Threat Defense（FTD）ソフトウェアに影響を及ぼさないことを確認しています。

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。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。

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

シスコは、Cisco ASAソフトウェアリリース9.13.1.16およびリリース9.14.1.15以降でこの脆弱性を修正しています。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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を確認していません。

出典

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssl-dos-7uZWwSEy

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	「修正済みリリース」にて、9.13.1.16 が入手可能になったことを反映しました。	修正済みリリース	Final	2020年10月27日
1.0	初回公開リリース	—	Interim	2020-OCT-22

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。