Cisco適応型セキュリティアプライアンスおよびFirepower Threat Defenseソフトウェアの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-tls-CWY6zXB
初公開日 : 2024-10-23 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : Yes
Cisco バグ ID : CSCwk74813 CSCwj92223

CVE-2024-20494

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)ソフトウェアおよびCisco Firepower Threat Defense(FTD)ソフトウェアのTLS暗号化機能の脆弱性により、認証されていないリモートの攻撃者がデバイスのリロードを突発的に引き起こし、その結果、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、TLS 1.3ハンドシェイク中の不適切なデータ検証に起因します。攻撃者は、TLS 1.3対応のリスニングソケットを介して、巧妙に細工されたTLS 1.3パケットを該当システムに送信することにより、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者は該当デバイスのリロードを引き起こし、その結果 DoS 状態が発生する可能性があります。

注：この脆弱性は、Cisco Adaptive Security Device Manager(ASDM)を使用してCisco ASAソフトウェアをアップグレードする際に、VPN HostScanの通信障害やファイル転送障害を引き起こし、デバイスの整合性に影響を与える可能性もあります。

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。本脆弱性に対処する回避策がいくつかあります。

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-tls-CWY6zXB

このアドバイザリは、2024年10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の一部です。これらのアドバイザリとリンクの一覧については、

『シスコイベントレスポンス：Cisco ASA、FMC、およびFTDソフトウェアに関するセキュリティアドバイザリ公開半年刊2024年10月』を参照してください。

該当製品

脆弱性のある製品

この脆弱性は、SSLリスニングソケットを備え、TLS 1.3プロトコルを許可するように設定されているデバイス上で実行されているCisco ASAソフトウェアおよびFTDソフトウェアに影響を与えます。

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。

デバイスがTLSパケットを処理できるかどうかを確認する

Cisco ASAソフトウェアまたはFTDソフトウェアを実行しているデバイスがTLSパケットを処理できるかどうかを確認するには、show asp table socket | include SSLコマンドを使用して、任意のTCPポートでSSLリスニングソケットを探します。次の例は、TCPポート443および8443でSSLリスニングソケットを使用するCisco ASAデバイスの出力を示しています。

```
<#root>

ciscoasa#

show asp table socket | include SSL


SSL       00185038  LISTEN     172.16.0.250:

443

    0.0.0.0:*
SSL       00188638  LISTEN      10.0.0.250:

8443

    0.0.0.0:*
```

次の表では、左の列に、通信にTLSを使用するソフトウェア機能を示します。右側の列に示す各機能の基本設定は、show running-config CLI コマンドを実行すると表示されます。これらの機能により、SSLリスニングソケットが有効になる可能性があります。

ソフトウェア機能	脆弱性の可能性がある設定
HTTPサーバが有効[1、2]	`http server enable` `http`

ソフトウェア機能	脆弱性の可能性がある設定
SSL VPN[3]	webvpn enable

1. 管理Webサーバは、 httpコマンドで設定された範囲のIPアドレスからアクセスされる場合にのみ、この脆弱性の影響を受けます。
2. Cisco FTDソフトウェアでは、Cisco Secure Firewall Management Center(FMC)（以前のFirepower Management Center）の Devices > Platform Settings > HTTP AccessでHTTP機能が有効になっています。
3. Cisco FTDソフトウェアの場合、リモートアクセスVPN機能は、Cisco FMCソフトウェアの Devices > VPN > Remote Access、またはCisco Firepower Device Manager(FDM)の Remote Access VPNで有効になっています。

ソフトウェア設定でのTLSバージョンの識別

Cisco ASAソフトウェアまたはFTDソフトウェアを実行しているデバイスで、TLS 1.3が接続に使用できるかどうかを確認するには、次の例のように、show running-config all ssl CLIコマンドを使用してTLSの最小および最大バージョンを表示します。

<#root>

```
ciscoasa> enable
ciscoasa# show running-config all ssl

ssl server-version tlsv1.2 dtlsv1.2


ssl client-version tlsv1.2

ssl server-max-version tlsv1.3


.
.
.
```

ssl server-version設定がある場合、その設定によって、ネゴシエーション中にデバイスが使用する最小のTLSプロトコルバージョンが決まります。前記の例では、最小のTLSバージョンとしてtlsv1.2が設定されています。

存在する場合、ssl server-max-version設定によって、ネゴシエーション時にデバイスで使用される最も高いTLSプロトコルバージョンが決定されます。前記の例では、デバイスはtlsv1.3までのTLSプロトコルバージョンを受け入れます。その結果、デバイスはこの脆弱性の影響を受

けます。

ssl server-max-versionコマンドが出力に表示されない場合、クライアントとデバイスの間で使用可能な最も高いTLSバージョンがネゴシエート可能であり、デバイスはこの脆弱性の影響を受けます。

注： ssl server-max-versionがtlsv1.3よりも低い場合、そのデバイスはこの脆弱性の影響を受けません。この回避策は必要ないか、すでに適用されている可能性があります。

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 FMC ソフトウェアには影響を与えないことを確認しました。

回避策

該当デバイスで、ssl server-max-version コマンドをサポートするCisco ASAソフトウェアまたはFTDソフトウェアリリースが実行されている場合、管理者はこの脆弱性の回避策としてTLS 1.3を無効にすることができます。

注：CLIコマンドssl server-max-versionは、Cisco ASAソフトウェアリリース9.19.1.24および9.20.2とCisco FTDソフトウェアリリース7.4.1でサポートされています。

Cisco ASAソフトウェアでのTLS 1.3の無効化

Cisco ASAソフトウェアでTLS 1.3を無効にするには、次の例に示すように、ssl server-version およびssl server-max-version コマンドを使用して、TLSの最小および最大バージョンをTLS 1.2に設定します。

```
<#root>

ciscoasa# configure terminal
ciscoasa(config)#

ssl server-version tlsv1.2 dtlsv1.2


ciscoasa(config)#

ssl server-max-version tlsv1.2
```

Cisco FTDソフトウェアのTLS 1.3を無効にする

Cisco FTDソフトウェアのTLS 1.3を無効にするには、Cisco FMCソフトウェアとFlexConfigオブジェクトを使用して、最小および最大のTLSバージョンをTLS 1.2に設定します。FlexConfigオブジェクトの詳細については、『Firepower Management Centerコンフィギュレーションガイド』の「FTDのFlexConfigポリシー」の章を参照してください。

Cisco FTDソフトウェアでTLS 1.3を無効にするには、次の手順を使用します。

1. Cisco FMCソフトウェアに接続する
2. メニューバーからDevices > Platform Settingsの順に選択します。
3. 影響を受けるデバイスに適用されるプラットフォーム設定ポリシーを追加または編集します。
4. 左側のナビゲーションメニューから、SSLを選択します。
5. TLS versionドロップダウンメニューから、TLSv1.2を選択します。
6. [Save] をクリックします。
7. Objects > Object Managementの順に選択します。
8. 左側のナビゲーションメニューから、FlexConfig > FlexConfig Objectを選択します。
9. Add FlexConfig Objectをクリックします。
10. 適切なフィールドにオブジェクトの名前と説明（オプション）を入力します。
11. メインテキストボックスの上にあるドロップダウンメニューから、Insert、Deployment: Once、Type: Appendの順に選択します。
12. メインテキストボックスにss server-max-version tlsv1.2と入力します。
    注：語ssの最後にlは付いていません。これは、入力ミスではありません。単語sslが使用されている場合、変更が保存されるとCisco FMCソフトウェアで検証エラーが表示されます。
13. [Save] をクリックします。
14. メニューバーからDevices > FlexConfigの順に選択します。
15. 既存のFlexConfigポリシーを編集するか、新しいポリシーを追加します。新しいポリシーを追加する場合は、新しいポリシーの名前と説明（オプション）を該当するフィールドに入力し、Saveをクリックします。
16. 左側のUser Definedドロップダウンメニューから、ステップ9で追加したFlexConfigオブジェクトを選択します。
17. >をクリックして、オブジェクトをSelected Append FlexConfigsペインに移動します。
18. [Save] をクリックします。
19. メニューバーからDeployをクリックして、変更を展開します。
20. ポリシーに割り当てられているデバイスのチェックボックスをオンにします。
21. ignore warningsチェックボックスにチェックマークを付けます。
    注： FlexConfigオブジェクトを配置する際に、警告を無視するチェックボックスがオンになるまで、検証警告が表示されないようにします。
22. ダイアログボックスでDeployをクリックします。

この回避策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において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

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。

Cisco ASA、FMC、および FTD ソフトウェア

お客様が Cisco ASA、FMC、および FTD ソフトウェアの脆弱性に対するリスクを判断できるように、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべての脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。または、次のフォームを使用して、特定のソフトウェアリリースに影響を及ぼす脆弱性を検索します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。すべてのアドバイザリ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、またはこのアドバイザリのみを選択します。
2. 該当するソフトウェアを選択します。
3. 該当するプラットフォームを選択します。
4. リリース番号を入力します。たとえば、Cisco ASA ソフトウェアの場合は 9.16.2.11、Cisco FTD ソフトウェアの場合は 6.6.7 と入力します。
5. [チェック（Check）] をクリックします。

2		Critical,High,Medium
このアドバイザのみ	Cisco ASA ソフトウェア	
あらゆるプラットフォーム		
Enter release number	Check	

注：Cisco ASAソフトウェアを実行しているCisco 3000シリーズ産業用セキュリティアプライアンス(ISA)については、Cisco ASAソフトウェアリリース9.16.4.67のリリースは延期されており、リリース9.16.4.70に置き換えられています。

Cisco FTDデバイスのアップグレード手順については、該当する『Cisco FMC upgrade guide』を参照してください。

関連情報

最適な Cisco ASA、FMC、または FTD ソフトウェアリリースの決定方法については、次の推奨リリースに関するドキュメントを参照してください。セキュリティ アドバイザリでより新しいリリースが推奨されている場合は、そのアドバイザリのガイダンスに従うことをお勧めします。

Cisco ASA の互換性
Cisco Secure Firewall ASA アップグレードガイド
Cisco Secure Firewall Threat Defense 互換性ガイド

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 、シスコ内部でのセキュリティテスト中に Ilkin Gasimov によって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-tls-CWY6zXB

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10月23日

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。