Cisco ASA および FTD ソフトウェアの暗号化 TLS と SSL ドライバで確認されたサービス妨害の脆弱性

High

アドバイザリーID : cisco-sa-20190710-asa-ftd-dos
CVE-2019-1873
初公開日 : 2019-07-10 16:00
最終更新日 : 2019-07-11 21:11
バージョン 1.1 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCvp36425

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）および Firepower Threat Defense（FTD）ソフトウェアの暗号化ドライバで脆弱性が確認されました。認証されていないリモートの攻撃者が、デバイスの予期せぬ再起動を引き起こす危険性があります。

この脆弱性は、セキュア ソケット レイヤ（SSL）または Transport Layer Security（TLS）の着信パケット ヘッダーの入力検証が不完全であることに起因します。攻撃者が、細工した TLS/SSL パケットを標的デバイスのインターフェイスに送信することで、この脆弱性がエクスプロイトされる可能性があります。エクスプロイトによりデバイスのリロードが実行されると、サービス妨害（DoS）状態に陥る危険性があります。

注：本脆弱性を不正利用する目的で使用できるのは、該当システム宛てのトラフィックに限られます。この脆弱性は、シングルまたはマルチ コンテキスト モードにおいて、ルーティング モードおよびトランスペアレント ファイアウォール モードに設定されたシステムに影響します。また、この脆弱性は、IPv4 トラフィックと IPv6 トラフィックでトリガーされる可能性があります。この脆弱性のエクスプロイトには、有効な SSL または TLS セッションが必要です。

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-

20190710-asa-ftd-dos

該当製品

脆弱性のある製品

脆弱性の影響を受けるのは、次のシスコ製品で脆弱性のある Cisco ASA ソフトウェアまたは FTD ソフトウェア リリースを実行している場合です。

- ASA 5506-X
- ASA 5506-X with FirePOWER サービス
- ASA 5506H-X
- ASA 5506H-X with FirePOWER サービス
- ASA 5506W-X
- ASA 5506W-X with FirePOWER サービス
- ASA 5508-X
- ASA 5508-X with FirePOWER サービス
- ASA 5516-X
- ASA 5516-X with FirePOWER サービス

SSL および TLS パケットの復号化と暗号化で、特定の暗号化ドライバが使用される ASA ハードウェア プラットフォームのみが影響を受けます。Cisco ASA ソフトウェアまたは FTD ソフトウェアのの機能は、有効にすると SSL/TLS パケット処理を実行します。これらの機能には次のようなものがあります。

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

Cisco ASA ソフトウェアまたは FTD ソフトウェアを実行中のデバイスで、SSL または TLS パケットが処理され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。このコマンドで返される出力が空の場合、そのデバイスに脆弱性はありません。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>

BSNS-ASA5505-4#

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。

- 3000 シリーズ産業用セキュリティ アプライアンス（ISA）
- 7600 シリーズ ASA サービス モジュール
- 適応型セキュリティ仮想アプライアンス（ASAv）
- ASA 1000V クラウド ファイアウォール
- ASA 5505 適応型セキュリティ アプライアンス
- ASA 5510 適応型セキュリティ アプライアンス
- ASA 5512-X 適応型セキュリティ アプライアンス
- ASA 5515-X 適応型セキュリティ アプライアンス
- ASA 5520 適応型セキュリティ アプライアンス
- ASA 5525-X 適応型セキュリティ アプライアンス
- ASA 5540 適応型セキュリティ アプライアンス
- ASA 5545-X 適応型セキュリティ アプライアンス
- ASA 5550 適応型セキュリティ アプライアンス
- ASA 5555-X 適応型セキュリティ アプライアンス
- ASA 5580 適応型セキュリティ アプライアンス
- ASA 5585-X 適応型セキュリティ アプライアンス
- ASA 5512-X with FirePOWER サービス
- ASA 5515-X with FirePOWER サービス
- ASA 5525-X with FirePOWER サービス
- ASA 5545-X with FirePOWER サービス
- ASA 5555-X with FirePOWER サービス
- ASA 5585-X with FirePOWER SSP-10、SSP-20、SSP-40、または SSP-60
- Catalyst 6500 シリーズ ASA サービス モジュール
- Firepower 2100 シリーズ
- Firepower 4100 シリーズ
- FirePOWER 7000 シリーズ アプライアンス
- FirePOWER 8000 シリーズ アプライアンス
- Firepower 9300 セキュリティ アプライアンス
- Firepower Threat Defense Virtual（FTDv）
- Industrial Security Appliance 3000

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 https://www.cisco.com/c/en/us/products/end-user-license-agreement.html に記載の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。

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、[シスコのセキュリティアドバイザリおよびアラート（Cisco Security Advisories and Alerts）] 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完全なアップグレード ソリューション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 Cisco Service Contract 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 POS から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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

この項の該当する表に示すように、適切なリリースにアップグレードすることをお勧めします。

次の表では、左の列に Cisco ソフトウェアのリリースを示します。右の列は、そのリリースが本アドバイザリに記載した脆弱性に該当するかどうか、また、本脆弱性に対処するための修正を含むリリースを示します。

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
9.4 より前[1]	9.4.4.36
9.4	9.4.4.36
9.51	9.6.4.29
9.6	9.6.4.29
9.7[1]	9.8.4.3
9.8	9.8.4.3
9.9	9.9.2.52
9.10	9.10.1.22
9.12	9.12.2

1 Cisco ASA ソフトウェアの 9.4 より前のリリース、Cisco ASA ソフトウェア リリース 9.5、および 9.7 については、メンテナンスが終了しています。この脆弱性に対する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。

Cisco FTD ソフトウェア

Cisco FTD 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
6.0[1]	6.2.3.13
6.0.1[1]	6.2.3.13
6.1.0	6.2.3.13
6.2.0	6.2.3.13
6.2.1	6.2.3.13
6.2.2	6.2.3.13
6.2.3	6.2.3.13
6.3.0	Cisco_FTD_Hotfix_AA-6.3.0.4-2または6.3.0.4（2019年8月）
6.4.0	6.4.0.2

1Cisco FTD ソフトウェアの 6.0.1 以前のリリースは、メンテナンスが終了しています。この脆弱性に対する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。

Cisco FTD ソフトウェアの修正済みリリースにアップグレードするには、次のいずれかの操作を行います。

- Cisco Firepower Management Center（FMC）を使用して管理しているデバイスについては、FMC インターフェイスを使用してアップグレードをインストールします。インストールが完了したら、アクセス コントロール ポリシーを再適用します。
- Cisco Firepower Device Manager（FDM）を使用して管理しているデバイスについては、FDM インターフェイスを使用してアップグレードをインストールします。インストールが完了したら、アクセス コントロール ポリシーを再適用します。

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-20190710-asa-ftd-dos

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	FTD 6.3.0リリースのホットフィックス情報を追加。	修正済みソフトウェア	Final	2019年7月11日
1.0	初回公開リリース	—	Final	2019 年 7 月 10 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。