Firepower 3100 および 4200 シリーズ 向け Cisco Secure Firewall 適応型セキュリティアプライアンスおよび Cisco Secure Firewall Threat Defense の各ソフトウェアの TLS 1.3 暗号におけるサービス妨害（DoS）脆弱性

アドバイザリーID : cisco-sa-3100_4200_tlsdos-2yNSCd54
初公開日 : 2025-08-14 16:00
最終更新日 : 2025-09-03 13:37
バージョン 1.1 : Final
CVSSスコア : 7.7
回避策 : Yes
Cisco バグ ID : CSCwm91176

CVE-2025-20127

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 Firepower 3100 および 4200 シリーズ デバイス向け Cisco Secure Firewall 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 Secure Firewall Threat Defense（FTD）ソフトウェアの特定の暗号に対する TLS 1.3 の実装における脆弱性により、認証されたリモートの攻撃者によって着信 TLS 1.3 接続に関連付けられたリソースが消費される可能性があります。これによって、最終的にデバイスが新しい SSL/TLS または VPN のリクエストを受け入れなくなる可能性があります。

この脆弱性は、TLS 1.3 暗号 TLS_CHACHA20_POLY1305_SHA256 の実装に起因します。特定の TLS 1.3 暗号 TLS_CHACHA20_POLY1305_SHA256 で多数の TLS 1.3 接続を送信することで、攻撃者がこの脆弱性をエクスプロイトする可能性があります。エクスプロイトが成功すると、攻撃者によってサービス妨害（DoS）状態が引き起こされ、新たに着信する暗号化接続が受け入れられなくなる可能性があります。この状態を解消するには、デバイスをリロードする必要があります。

注：これらの着信 TLS 1.3 接続には、データトラフィックとユーザー管理トラフィックの両方が含まれます。デバイスが脆弱な状態になると、新しい暗号化接続を受け入れることができなくなります。

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。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-3100_4200_tlsdos-2yNSCd54

このアドバイザリは、2025 年 8 月に公開された Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェアのセキュリティ 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: August 2025 Semiannual Cisco Secure Firewall ASA, Secure FMC, and Secure FTD Software Security Advisory Bundled Publication』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 暗号 TLS_CHACHA20_POLY1305_SHA256 を許可するように設定されている Cisco Secure Firewall 3100 または 4200 シリーズ のデバイスで実行されている Cisco Secure Firewall ASA ソフトウェアおよび Cisco Secure FTD ソフトウェアに影響を与えます。これはデフォルト設定ではありません。

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。

デバイスが TLS パケットを処理できるかどうかの確認

Cisco Secure Firewall ASA ソフトウェアまたは Cisco Secure 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、すべての TCP ポートで SSL リスニングソケットを検索します。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 Secure Firewall 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:*
```

脆弱な TLS 1.3 暗号ソフトウェア設定の特定

デバイスがこの脆弱性の影響を受けるのは、TLS 1.3 暗号 TLS_CHACHA20_POLY1305_SHA256 が設定されている場合のみです。Cisco Secure Firewall ASA ソフトウェアまたは Cisco Secure FTD ソフトウェアを実行しているデバイスに TLS 1.3 暗号 TLS_CHACHA20_POLY1305_SHA256 が設定されているかどうかを確認するには、show running-config all ssl | include TLS_CHACHA20_POLY1305_SHA256 CLI コマンドを使用します。次の例に示すような出力が返される場合、デバイスに脆弱性があると判断されます。

```
<#root>
ciscoasa#
show running-config all ssl | include TLS_CHACHA20_POLY1305_SHA256

ssl cipher tlsv1.3 custom "TLS_CHACHA20_POLY1305_SHA256"
```

また、次の例に示すように、ssl cipher tlsv1.3 high、ssl cipher tlsv1.3 medium、またはssl cipher tlsv1.3 lowがshow running-config ssl | include tlsv1.3の下に存在する場合、TLS 1.3暗号TLS_CHACHA20_POLY1305_SHA256を暗号として設定できます。

```
<#root>
ciscoasa#
show running-config all ssl | include tlsv1.3

ssl cipher tlsv1.3
 medium
```

この場合、管理者はshow ssl ciphers medium | include v1.3コマンドを使用して、次の例のようにTLS_CHACHA20_POLY1305_SHA256が設定されているかどうかを確認する必要があります。

```
<#root>
```

```
ciscoasa#
show ssl ciphers medium | include v1.3

 TLS_AES_128_GCM_SHA256 (tlsv1.3)

TLS_CHACHA20_POLY1305_SHA256
 (tlsv1.3)
 TLS_AES_256_GCM_SHA384 (tlsv1.3)
```

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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性が Cisco Secure Firewall Management Center（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。

セキュリティ侵害の痕跡

この脆弱性があると、デバイスでセキュリティ コンテキスト ブロック（SCB）ハンドルが使い果たされてしまいます。SCB ハンドルは、SSL、VPN、TLS、インターネット キー エクスチェンジ（IKE）など、すべての着信暗号化接続を処理するために使用されるものです。 次の 2 つの侵害の兆候を探してください。これらは、この脆弱性がエクスプロイトされた場合に現れる可能性のあるものです。

ログに記録された SSL エラー

show ssl errors CLI コマンドを実行すると、次のエラーが繰り返し表示される場合があります。

```
error:1424A044:SSL routines:write_state_machine:internal error@libssl_ext_hndshk_accel.c:87
error:1424A044:SSL routines:write_state_machine:internal error@libssl_ext_hndshk_accel.c:87
```

SSL エラーカウンタ

show counters | include HANDLE_ALLOC_FAILED で表示されるカウンタが、次の例に示すように急激に増加する場合があります。

```
<#root>

ciscoasa#
```

```
show counters | include HANDLE_ALLOC_FAILED

CRYPTO       HANDLE_ALLOC_FAILED                          56169
```

Summary

注：デバイスがこのような機能不全の状態になっている場合、接続を復元するには再起動が必要です。

回避策

この脆弱性に対処する回避策はありません。 no ssl cipher tlsv1.3 custom<cipher list> CLI コマンドを使用して暗号を削除します。

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 Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェア

お客様が Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェアにおける脆弱性のリスクの有無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、セキュリティへの影響の評価（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 Secure Firewall ASA ソフトウェアの場合は 9.20.3.4、Cisco Secure FTD ソフトウェアの場合は 7.4.2 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

Cisco Secure FTD デバイスのアップグレード手順については、該当の Cisco Secure FMC アップグレードガイドを参照してください。

関連情報

最適な Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各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 Secure Firewall 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 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-3100_4200_tlsdos-2yNSCd54

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	問題のある暗号の設定例を更新。	脆弱性が存在する製品	Final	2025年9月3日
1.0	初回公開リリース	—	Final	2025 年 8 月 14 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。