# Cisco 適応型セキュリティ アプライアンス ソフトウェアおよび Firepower Threat Defense ソフトウェアで確認された不正な OSPF パケット処理によるサービス妨害の脆弱性


アドバイザリーID : cisco-sa-asa-ftd-ospf-dos-RhMQY8qx
CVE-2020-3298
初公開日 : 2020-05-06 16:00
最終更新日 : 2020-06-02 20:50
バージョン 1.3 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCvs50459

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 Open Shortest Path First（OSPF）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該当デバイスのリロードを引き起こし、サービス妨害（DoS）状態に陥る可能性があります。

この脆弱性は、特定の OSPF パケット処理中の不適切なメモリ保護メカニズムに起因します。不正な OSPF パケットが短時間に連続して該当システムに送信されると、この脆弱性がエクスプロイトされる危険性があります。エクスプロイトに成功すると、攻撃者が該当デバイスをリロードできるようになり、その結果、デバイスを横断しているクライアントのトラフィックに対してサービス妨害（DoS）状態が発生する可能性があります。

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ソフトウェア アップデートを提供しています。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-ftd-ospf-dos-RhMQY8qx

このアドバイザリは、2020 年 5 月 に公開された Cisco ASA、FMC、FTD ソフトウェアのセキュリティ アドバイザリ バンドルの一部です。このアドバイザリバンドルには、12 件の脆弱性に関

する 12 件のシスコ セキュリティ アドバイザリが記載されています。アドバイザリの完全なリストとそのリンクについては、『Cisco Event Response: May 2020 Cisco ASA, FMC, and 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 ソフトウェアまたは Cisco FTD ソフトウェアリリースを実行しており、かつ OSPF ルーティングで LLS ブロック処理が有効になっている場合です。注：LLSブロック処理はデフォルトで有効になっています。

## OSPF ルーティングが ASA デバイスで設定されているかどうかの確認

管理者は show ospf 特権モードコマンドを使用して、OSPF ルーティングが ASA デバイスで設定されているかどうかを確認できます。出力が返されない場合、OSPF ルーティングは設定されていません。次の例では、デバイスが OSPF ルーティング用に設定されています。

```
<#root>

asa#

show ospf


Routing Process “ospf 2” with ID 10.1.89.2 and Domain ID 0.0.0.2
Supports only single TOS(TOS0) routes
Supports opaque LSA
.
.
.
```

## OSPF ルーティングが FTD デバイスで設定されているかどうかの確認

管理者は次のいずれかの方法で、OSPF ルーティングが FTD デバイスで設定されているかどうかを確認できます。

- Cisco Firepower Management Center（FMC）を使用して管理されているデバイスの場合は、[デバイス（devices）] > [デバイス管理（device Management）] を選択し、対象のデバイスを選択して、[ルーティング（Routing）] > [OSPF] を選択します。プロセス 1 またはプロセス 2 のいずれかにチェックマークが付いている場合、デバイスで OSPF が有効になっています。
- Cisco Firepower Device Manager（FDM）を使用して管理されているデバイスの場合は、[デバイス（Device）] > [詳細設定（Advanced Configuration）] > [設定の表示（View

Configuration ) ] > [スマート CLI ( Smart CLI ) ] > [ルーティング ( Routing ) ] の順に選択します。OSPFのタイプのオブジェクトがある場合は、デバイスで OSPF が有効になっています。

脆弱性が存在する Cisco ASA ソフトウェアおよび FTD 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。

### 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 ) ソフトウェアに影響を及ぼさないことを確認しました。

## 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。右の列は、リリースがこのバンドルに記載された何らかの脆弱性に該当するかどうか、およびそれらすべて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。

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 |
|---|---|---|
| 9.5[1] より前 | 脆弱性なし | 修正済みリリースに移行。 |
| 9.51 | 脆弱性なし | 修正済みリリースに移行。 |
| 9.6 | 9.6.4.40 | 修正済みリリースに移行。 |
| 9.7[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 | 9.8.4.17 | 9.8.4.20 |
| 9.9 | 9.9.2.66 | 9.9.2.67 |
| 9.10 | 9.10.1.37 | 9.10.1.40 |
| 9.12 | 9.12.3.7 | 9.12.3.9 |
| 9.13 | 9.13.1.7 | 9.13.1.10 |
| 9.14 | 脆弱性なし | 脆弱性なし |

1. Cisco ASA ソフトウェアリリース 9.5 以前および 9.7 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。

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 | 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 |
|---|---|---|
| 6.1.0[1] より前 | 脆弱性なし | 修正済みリリースに移行。 |
| 6.1.0 | 脆弱性なし | 修正済みリリースに移行。 |
| 6.2.0 | 脆弱性なし | 修正済みリリースに移行。 |
| 6.2.1 | 脆弱性なし | 修正済みリリースに移行。 |
| 6.2.2 | 脆弱性なし | 修正済みリリースに移行。 |
| 6.2.3 | 6.2.3.16（2020 年 6 月）<br>Cisco_FTD_Hotfix_DT-6.2.3.16-3.sh.REL.tar<br>Cisco_FTD_SSP_FP2K_Hotfix_DT-6.2.3.16-3.sh.REL.tar<br>Cisco_FTD_SSP_Hotfix_DT-6.2.3.16-3.sh.REL.tar | 6.2.3.16（2020 年 6 月）<br>Cisco_FTD_Hotfix_DT-6.2.3.16-3.sh.REL.tar<br>Cisco_FTD_SSP_FP2K_Hotfix_DT-6.2.3.16-3.sh.REL.tar<br>Cisco_FTD_SSP_Hotfix_DT-6.2.3.16-3.sh.REL.tar |
| 6.3.0 | 6.3.0.6（リリース予定）<br>Cisco_FTD_Hotfix_AO-6.3.0.6-2.sh.REL.tar<br>Cisco_FTD_SSP_FP2K_Hotfix_ AO-6.3.0.6-2.sh.REL.tar<br>Cisco_FTD_SSP_Hotfix_ AO-6.3.0.6-2.sh.REL.tar | 6.3.0.6（リリース予定）<br>Cisco_FTD_Hotfix_AO-6.3.0.6-2.sh.REL.tar<br>Cisco_FTD_SSP_FP2K_Hotfix_ AO-6.3.0.6-2.sh.REL.tar<br>Cisco_FTD_SSP_Hotfix_ AO-6.3.0.6-2.sh.REL.tar |
| 6.4.0 | 6.4.0.9 | 6.4.0.9 |
| 6.5.0 | 6.5.0.5（リリース予定）<br>Cisco_FTD_Hotfix_H-6.5.0.5-2.sh.REL.tar 以降<br>Cisco_FTD_SSP_FP1K_Hotfix_H-6.5.0.5-2.sh.REL.tar 以降<br>Cisco_FTD_SSP_FP2K_Hotfix_H-6.5.0.5-2.sh.REL.tar 以降<br>Cisco_FTD_SSP_Hotfix_H-6.5.0.5-2.sh.REL.tar 以降 | 6.5.0.5（リリース予定）<br>Cisco_FTD_Hotfix_H-6.5.0.5-2.sh.REL.tar 以降<br>Cisco_FTD_SSP_FP1K_Hotfix_H-6.5.0.5-2.sh.REL.tar 以降<br>Cisco_FTD_SSP_FP2K_Hotfix_H-6.5.0.5-2.sh.REL.tar 以降<br>Cisco_FTD_SSP_Hotfix_H-6.5.0.5-2.sh.REL.tar 以降 |
| 6.6.0 | 脆弱性なし | 6.6.0 |

1. Cisco FMC および FTD ソフトウェア リリース 6.0.1 以前については、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。

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、シスコ内部でセキュリティテストを実施中に、Santosh Krishnamurthy によって発見されました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-ospf-dos-RhMQY8qx

## 改訂履歴

| バージョン | 説明 | セクション | ステータス | 日付 |
|---|---|---|---|---|
| 1.2 | FTD リリース 6.4.0 および 6.5.0 の Hot Fix を更新。 | 修正済みリリース | Final | 2020 年 5 月 15 日 |
| 1.0 | 初回公開リリース | — | Final | 2020 年 5 月 6 日 |
| 1.3 | 修正済み FTD リリース 6.4.0 ソフトウェアのリリースに関する情報を更新。 | 修正済みリリース | Final | 2020 年 5 月 6 日 |
| 1.1 | 正しい修正済みリリースを 9.10.1.39 ではなく 9.10.1.40 とするために、ASA 修正リリーステーブルを更新。 | 修正済みリリース | Final | 2020 年 5 月 6 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。