# Cisco Secure Firewall適応型セキュリティアプライアンスおよびSecure Firewall Threat Defenseソフトウェアの OSPFプロトコルの脆弱性

Medium

アドバイザリーID : cisco-sa-asaftd-ospf-ZH8PhbSW
初公開日 : 2026-03-04 16:00
バージョン 1.0 : Final
CVSSスコア : 6.8
回避策 : No workarounds available
Cisco バグ ID : CSCwn69079 CSCwn69078 CSCwq73656 CSCwn69075 CSCwn69076 CSCwn69081 CSCwo71552

CVE-2026-20024
CVE-2026-20025
CVE-2026-20022
CVE-2026-20023
CVE-2026-20020
CVE-2026-20021

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 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OSPF機能における複数の脆弱性により、隣接する攻撃者がデバイスの予期せぬリロードを引き起こし、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。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコはこれら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。これら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-asaftd-ospf-ZH8PhbSW

このアドバイザリは、2026年3月に公開された『Cisco Secure Firewall ASA、Secure FMC、およ

びSecure 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。アドバイザリとリンクの一覧については、『Cisco Event Response: March 2026 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

公開時点では、これらの脆弱性は、OSPFプロトコルを実行しているCisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアに影響を与えました。

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。

### 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、これら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、これらの脆弱性が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。

## 詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェアリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2026-20020:Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのOSPF DoS脆弱性

Cisco Secure Firewall ASAソフトウェアおよびCisco Secure FTDソフトウェアのOSPFプロトコルの脆弱性により、認証されていない隣接する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、その結果、DoS状態が発生する可能性があります。OSPF認証が有効になっている場合、攻撃者がこの脆弱性を悪用するには秘密鍵を知っている必要があります。

この脆弱性は、OSPF更新パケットを処理する際の不十分な入力検証に起因します。攻撃者は、巧妙に細工されたOSPF更新パケットを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。エクスプロイトに成功すると、攻撃者はバッファオーバーフローを作成し、影響を受ける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。

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。

バグID: CSCwn69076
CVE ID：CVE-2026-20020
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.8
CVSSベクトル：CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

CVE-2026-20024:Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのOSPFヒープ破損の脆弱性

Cisco Secure Firewall ASAソフトウェアおよびCisco Secure FTDソフトウェアのOSPFプロトコルの脆弱性により、認証された隣接する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、その結果、DoS状態が発生する可能性があります。この脆弱性を不正利用するには、攻撃者はOSPF秘密鍵を持っている必要があります。

この脆弱性は、パケット解析時のOSPFのヒープ破損に起因します。攻撃者は、巧妙に細工されたパケットをOSPFサービス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。エクスプロイトに成功すると、攻撃者がヒープを破損し、影響を受けるデバイスがリロードされ、DoS状態が発生する可能性があります。

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。この脆弱性に対処する回避策はありません。

バグID: CSCwn69075
CVE ID：CVE-2026-20024
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.8
CVSSベクトル：CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

CVE-2026-20025:Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのOSPF DoS脆弱性

Cisco Secure Firewall ASAソフトウェアおよびCisco Secure FTDソフトウェアのOSPFプロトコルの脆弱性により、認証された隣接する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、その結果、DoS状態が発生する可能性があります。この脆弱性を不正利用するには、攻撃者はOSPF秘密鍵を持っている必要があります。

この脆弱性は、OSPFリンクステートアップデート(LSU)パケットを処理する際の不十分な入力検証に起因します。攻撃者は、巧妙に細工されたOSPF LSUパケットを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。エクスプロイトに成功すると、攻撃者がヒープを破損し、デバイスがリロードされ、DoS状態が発生する可能性があります。

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。この脆弱性に

対処する回避策はありません。

バグID: CSCwn69078
CVE ID：CVE-2026-20025
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.8
CVSSベクトル：CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

CVE-2026-20022:Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのOSPF DoS脆弱性

Cisco Secure Firewall ASAソフトウェアおよびCisco Secure FTDソフトウェアのOSPFプロトコルの脆弱性により、認証されていない隣接する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、debug ip ospf canonコマンドを使用してOSPF正規化のデバッグを有効にすると、DoS状態が発生する可能性があります。

この脆弱性は、OSPF LSUパケットを処理する際の不十分な入力検証に起因します。攻撃者は、巧妙に細工された非認証OSPFパケットを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。エクスプロイトに成功すると、攻撃者はパケットデータの外部のメモリに書き込みを行い、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。

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。

バグID: CSCwo71552、CSCwn69081
CVE ID：CVE-2026-20022
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.1
CVSSベクトル：CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H

CVE-2026-20023:Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのOSPFメモリ破損の脆弱性

Cisco Secure Firewall ASAソフトウェアおよびCisco Secure FTDソフトウェアのOSPFプロトコルの脆弱性により、認証されていない隣接する攻撃者が該当デバイスのメモリを破損させ、その結果DoS状態が発生する可能性があります。

この脆弱性は、OSPFプロトコルパケットを解析する際のメモリ破損に起因します。攻撃者は、巧妙に細工されたOSPFパケットを該当デバイス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。エクスプロイトに成功すると、攻撃者はメモリを破損させ、影響を受けるデバイスをリブートさせ、その結果DoS状態を引き起こす可能性があります。

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。この脆弱性に対処する回避策はありません。

バグID: CSCwq73656
CVE ID：CVE-2026-20023
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.1
CVSSベクトル：CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H

CVE-2026-20021:Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアのOSPFメモリ枯渇の脆弱性

Cisco Secure Firewall ASAソフトウェアおよびCisco Secure FTDソフトウェアのOSPFプロトコルの脆弱性により、認証されていない隣接する攻撃者が該当デバイスのメモリを枯渇させ、DoS状態を引き起こす可能性があります。

この脆弱性は、OSPFプロトコルパケットを処理する際の不十分な入力検証に起因します。攻撃者は、巧妙に細工されたOSPFパケットを該当デバイス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。エクスプロイトに成功すると、攻撃者は該当デバイスのメモリを枯渇させ、DoS状態を引き起こす可能性があります。

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。この脆弱性に対処する回避策はありません。

バグID: CSCwn69079
CVE ID：CVE-2026-20021
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.3
CVSS ベクトル：CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

## 回避策

これら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

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。これらの脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

### 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）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例とその公表は確認しておりません。

## 出典

これらの脆弱性は、Cisco Advanced Security Initiatives Group（ASIG）の Jason Crowder による内部セキュリティテストで発見されました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ospf-ZH8PhbSW

## 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 | 2026年3月4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。