複数のシスコ製品におけるSnort 3のDoS脆弱性

Medium

アドバイザリーID : cisco-sa-snort3-multi-dos-XFWkWSwz
初公開日 : 2026-03-04 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : No workarounds available
Cisco バグ ID : CSCwq97624 CSCwn65473 CSCwq01529 CSCwq97644 CSCwn49805 CSCwp99280 CSCwq03411 CSCwq23374 CSCwq82404 CSCwq01530 CSCwo93208 CSCwo93207 CSCwr21398 CSCwq97649

CVE-2026-20005
CVE-2026-20068
CVE-2026-20066
CVE-2026-20067
CVE-2026-20065

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

Snort 3検出エンジンの脆弱性により、認証されていないリモートの攻撃者がSnort 3検出エンジンの再起動を引き起こし、その結果、パケットインスペクションの中断が発生する可能性がある複数のシスコ製品が影響を受けます。

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-snort3-multi-dos-XFWkWSwz

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

公開時点でこれらの脆弱性の影響を受けた製品については、次のセクションを参照してください。

オープンソースの Snort 3

公開時点で、これらの脆弱性はOpen Source Snort 3に影響を与えました。

公開時点で脆弱性が存在するSnort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。Snortの詳細については、Snort Webサイトを参照してください。

Cisco Secure Firewall Threat Defenseソフトウェア

公開時点で、Snort 3が設定されている場合、これらの脆弱性はCisco Secure Firewall Threat Defense(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。

Cisco Secure FTD ソフトウェアの Snort 設定の確認

Cisco Secure FTDソフトウェアリリース7.0.0以降の新規インストールでは、Snort 3がデフォルトで実行されます。Cisco Secure FTDソフトウェアリリース6.7.0以前を実行していて、リリース7.0.0以降にアップグレードされたデバイスでは、デフォルトでSnort 2が実行されます。

Cisco Secure FTD ソフトウェアで Snort 3 が実行されているかどうかを確認するには、「Firepower Threat Defense（FTD）で実行されているアクティブな Snort バージョンの判別」を参照してください。 これらの脆弱性を不正利用するには、Snort 3がアクティブである必要があります。

Cisco IOS XE ソフトウェア

公開時点では、Cisco IOS XEソフトウェア用のUnified Threat Defense(UTD)Snort IPS Engine、またはCisco IOS XE SD-WANソフトウェア用のUTD Engineの脆弱性のあるリリースを実行する次のシスコ製品がこの脆弱性の影響を受けました。

- 1000 シリーズ サービス統合型ルータ（ISR）
- 4000 シリーズ ISR
- 8100 シリーズ セキュアルータ
- 8200 シリーズ セキュアルータ
- 8300 シリーズ セキュアルータ

- 8400 シリーズ セキュアルータ
- Catalyst 8000V エッジソフトウェア
- Catalyst 8200 シリーズ エッジ プラットフォーム
- Catalyst 8300 シリーズ エッジ プラットフォーム
- Catalyst 8500L エッジプラットフォーム
- Catalyst IR1800高耐久性シリーズルータ
- Catalyst IR8340高耐久性ルータ
- クラウドサービスルータ 1000V
- サービス統合型仮想ルータ

注：UTDはデフォルトではこれらのデバイスにインストールされていません。UTDファイルがインストールされていない場合、デバイスはこれらの脆弱性の影響を受けません。

このアドバイザリの公開時点で脆弱性が存在するシスコ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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

UTD が有効かどうかを確認する方法

デバイスでUTDが有効になっているかどうかを確認するには、show utd engine standard statusコマンドを使用します。出力のRunningの下にYesと表示されている場合、UTDは有効です。出力が表示されない場合、デバイスは影響を受けていません。次の例は、UTDが有効になっているデバイスでの出力を示しています。

```
<#root>

Router#

show utd engine standard status


Engine version        : 1.0.19_SV2.9.16.1_XE17.3
Profile               : Cloud-Low
System memory         :
             Usage  : 6.00 %
             Status : Green
Number of engines     : 1
```

```
<#root>

Engine

Running

    Health     Reason
=========================================
```

```
Engine(#1):
Yes
        Green       None
=====================================================
.
.
.
```

Cisco Meraki製品への影響

公開時点では、CVE-2006-20005で説明されている脆弱性は、Merakiソフトウェアの脆弱性のあるリリースを実行している次の製品に影響を与えました。

• MX64 • MX64W • MX65 • MX65W • MX67 • MX67C • MX67W	• MX68 • MX68CW • MX75 • MX84 • MX85 • MX95	• MX100 • MX105 • MX250 • MX400 • MX450 • MX600

他のシスコ製品への影響

公開時点では、CVE-2006-20005、CVE-2026-20067、およびCVE-2026-20068で説明されている脆弱性がCisco Cyber Visionに該当していました。

このアドバイザリの公開時点で脆弱性が存在するシスコ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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細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。

また、シスコは、これらの脆弱性が以下の製品には影響を与えないことを確認しました。

- Cisco Secure Access Secure Internet Access(SIA)の利点
- Cisco Secure Access Secure Private Access(SPA)の利点
- 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

- Cisco Secure Firewall Management Center（FMC）ソフトウェア
- Cisco Umbrella Cloud-delivered Firewall(CDFW)(旧称Umbrella Secure Internet Gateway(SIG))
- オープンソースの Snort 2

シスコは、CVE-2006-20065、CVE-2026-20066、CVE-2026-20067、およびCVE-2026-20068がCisco Meraki製品に影響を与えないことを確認しました。

また、CVE-2006-20065およびCVE-2026-20066がCisco Cyber Visionに影響を与えないことも確認しました。

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-2026-20005：複数のシスコ製品におけるSnort 3 SSLのDoS脆弱性

Snort 3検出エンジンの脆弱性により、認証されていないリモートの攻撃者がSnort 3検出エンジンを再起動させ、パケットインスペクションの中断を引き起こす可能性がある複数のシスコ製品が影響を受けます。

この脆弱性は、Snort 3検出エンジンによるSSLハンドシェイク入力パケットの解析が不完全であることに起因します。攻撃者は、巧妙に細工されたSSLハンドシェイクパケットを送信することで、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、Snort 3検出エンジンが予期せず再起動したときに、サービス拒否(DoS)状態が引き起こされる危険性があります。

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: CSCwn65473 およびCSCwp99280
CVE ID：CVE-2026-20005
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L

CVE-2026-20065：複数のシスコ製品におけるSnort 3のバインダに関するDoS脆弱性

Snort 3検出エンジンの脆弱性により、認証されていないリモートの攻撃者がSnort 3検出エンジンを再起動させ、パケットインスペクションの中断を引き起こす可能性がある複数のシスコ製品が影響を受けます。

この脆弱性は、Snort検出エンジンのバインダーモジュール初期化ロジックのエラーが原因で発生します。攻撃者は、Snort 3によって解析される確立された接続を介して特定のパケットを送信することで、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、Snort 3検出エンジンが予期せず再起動したときに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: CSCwn49805
CVE ID：CVE-2026-20065
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L

CVE-2026-20066：複数のシスコ製品におけるSnort 3 JSTokenizerのDoS脆弱性

Snort 3検出エンジンの脆弱性により、認証されていないリモートの攻撃者がSnort 3検出エンジンを再起動させ、パケットインスペクションの中断を引き起こす可能性がある複数のシスコ製品が影響を受けます。

この脆弱性は、HTTPインスペクションでJavaScriptが正規化される際のJSTokenizer正規化ロジックのエラーに起因します。攻撃者は、Snort 3によって解析される確立された接続を介して巧妙に細工されたHTTPパケットを送信することで、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、Snort 3検出エンジンが予期せず再起動したときにDoS状態を引き起こす可能性があります。JSTokenizerはデフォルトでは有効になっていません。

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: CSCwq23374
CVE ID：CVE-2026-20066
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L

CVE-2026-20067：複数のシスコ製品におけるSnort 3マルチキャストDNSのDoS脆弱性

Snort 3検出エンジンの脆弱性により、認証されていないリモートの攻撃者がSnort 3検出エンジンを再起動させ、パケットインスペクションの中断を引き起こす可能性のある複数のシスコ製品が影響を受けます。

この脆弱性は、HTTPヘッダーのマルチキャストDNSフィールドを解析する際の不完全なエラーチェックに起因します。攻撃者は、確立された接続を介して巧妙に細工されたHTTPパケットを送信し、Snort 3によって解析されることで、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、Snort 3検出エンジンが予期せず再起動したときに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: CSCwq01530
CVE ID：CVE-2026-20067
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L

CVE-2026-20068：複数のシスコ製品でのSnort 3 RPCに関するDoS脆弱性

Snort 3検出エンジンの脆弱性により、認証されていないリモートの攻撃者がSnort 3検出エンジンを再起動させ、パケットインスペクションの中断を引き起こす可能性のある複数のシスコ製品が影響を受けます。

この脆弱性は、リモートプロシージャコール(RPC)データを解析する際の不完全なエラーチェックに起因します。攻撃者は、確立された接続を介して巧妙に細工されたRPCパケットを送信し、Snort 3によって解析されることで、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、Snort 3検出エンジンが予期せず再起動したときに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: CSCwq01529
CVE ID：CVE-2026-20068
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/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。

修正済みリリース

修正済みリリースの詳細については、次の項を参照してください。

オープンソースSnortソフトウェア

発行時点では、次の表に示すリリース情報は正確でした。

Snort 3リリース	CVE-2026-20005およびCVE-2026-20068の最初の修正済みリリース	CVE-2026-20065の最初の修正済みリリース	CVE-2026-20066の最初の修正済みリリース	CVE-2026-20067の最初の修正済みリリース
3.x	3.9.2.0 以降	3.6.3.0 以降	3.9.7.0 以降	3.9.5.0 以降

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

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

その他のプラットフォーム

公開時点では、次の表のリリース情報は正確でした。

左の列にはシスコソフトウェアリリースが、右の列にはリリースがこのアドバイザリに記載された脆弱性の影響を受けるかどうか、およびこれらの脆弱性に対する修正を含むリリースが示されています。

Meraki MX セキュリティ アプライアンス

Snortは、Cisco Merakiセキュリティアプライアンスに、Merakiダッシュボードを通じて自動的に管理される脅威保護サービスの一部としてネイティブに統合されます。MerakiファームウェアまたはMerakiデバイス用Snort 3パッケージのダウンロードには、お客様の操作は必要ありません。2026年2月5日の時点で、このアドバイザリに記載されているオンラインでCisco Merakiダッシュボードに接続されているすべてのMerakiモデルは、Snort 3パッケージで自動的に更新されています。これにより、2026年2月の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公開に対するSnort 3のすべての脆弱性が修正されます。

UTDソフトウェア：CSCwo93207、CSCwq82404、CSCwr21398、CSCwq97644、CSCwq97624

Cisco IOS XE ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
17.12 より前	脆弱性なし
17.12	17.12.7（2026年3月）
17.15	17.15.5
17.18	17.18.3 (Apr 2026)

Cisco IOS XE ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
26.1	26.1.1（2026年3月）

サイバービジョン：CSCwo93208、CSCwq97649、CSCwq03411

Cisco Cyber Visionリリース	CVE-2006-20067、CVE-2026-20067、およびCVE-2026-20068の最初の修正済みリリース
5.3 より前	修正済みリリースに移行。
5.3	5.3.3

シスコの Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、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とその公表は確認しておりません。

出典

CVE-2026-20005およびCVE-2026-20065：これらの脆弱性は、Cisco Technical Assistance Center(TAC)のサポートケースの解決中に発見されました。

CVE-2026-20066、CVE-2026-20067、およびCVE-2026-20068：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中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-multi-dos-XFWkWSwz

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

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。