複数のシスコ製品におけるSnort 3のDoS脆弱性

Medium

Advisory ID : cisco-sa-snort3-misc-dos-6mB22qAK
初公開日 : 2026-10-21 16:00
注: : 2026-10-22 19:03
バージョン 1.1 : Final
CVSSスコア : 5.8
回避策 : No workarounds available
Cisco Bug ID : CSCwu51451 CSCwu51449 CSCwu53570 CSCwu23999 CSCwr25134

CVE-2026-76489
CVE-2026-20019
CVE-2026-20179
CVE-2026-20197

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

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、その結果サービス妨害(DoS)状態が発生する可能性があり、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-misc-dos-6mB22qAK

本アドバイザリは一連のアドバイザリの一部です。アドバイザリの完全なリストおよび各アドバイザリへのリンクについては、「Cisco Advance Notification for Publication of October 21, 2026, Security Advisories」を参照してください。さらに、オープンソースSnort 3の改善と修正に関するその他のドキュメントについては、『複数のシスコ製品に関するSnort 3セキュリティ強化リリース：2026年10月』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、オープンソースのSnort 3がNetflowプロトコル接続を解析するように設定されている場合、これらの脆弱性の影響を受けました。

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Netflowプロトコル接続を解析するように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 Secure 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。

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。

Snort 2は、Cisco Secure FTDソフトウェアリリース7.7.0以降では廃止されました。

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。 これらの脆弱性をエクスプロイトするには、Snort 3がアクティブである必要があります。

Cisco IOS XEソフトウェアでの統合脅威対策

公開時点で、これらの脆弱性は次のシスコ製品に影響を与えました。これらの製品では、脆弱性が存在するUnified Threat Defense(UTD)Snort IPS Engine for Cisco IOS XE SoftwareまたはUTD Engine for Cisco IOS XE SD-WAN Softwareリリースを実行している場合です。

- 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。

公開時点で脆弱性が存在するCisco IOS XE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。

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 MXセキュリティアプライアンス

公開時点で、これらの脆弱性は、Cisco Merakiソフトウェアの脆弱性のあるリリースを実行す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

Cisco Merakiダッシュボードに接続されているデバイスの自動アップグレードの詳細については、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、これらの脆弱性が以下の製品には影響を与えないことを確認しました。

- シスコのクラウド配信ファイアウォール(CDFW)
- Cisco Cyber Vision
- シスコセキュアアクセス(CSA)
- 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
- オープンソースの Snort 2

注：オープンソースのSnort 2は廃止されました。詳細については、「Open Source Snort 2のサポート終了のお知らせ」を参照してください。

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-2026-20019：複数のシスコ製品におけるSnort 3 NetflowのDoS脆弱性

Snort 3 NetFlow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がUDP Netflowプロトコルパケット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1つのNetflowパケットを送信し、Snort 3で解析することで、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検出エンジンを予期せず再起動させ、DoS状態を引き起こす可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID:CSCwu23999およびCSCwu53570
CVE ID：CVE-2026-20019
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-2026-20179：複数のシスコ製品におけるSnort 3の総称ルーティングカプセル化(GRE)に関するDoS脆弱性

Snort 3総称ルーティングカプセル化(GRE)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り、複数のシスコ製品が影響を受けます。

この脆弱性は、Snort 3がGREパケット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、巧妙に細工されたGREパケットをターゲットデバイスに送信してSnortによって解析され、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検出エンジンを予期せず再起動させ、DoS状態を引き起こす可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: CSCwu51449
CVE ID：CVE-2026-20179
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-2026-20197：複数のシスコ製品におけるSnort 3 TeredoプロトコルのDoS脆弱性

Snort 3 Teredo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がTeredoパケット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、巧妙に細工されたTeredoパケットをターゲットデバイスに送信してSnortによって解析されることにより、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Snort 3検出エンジンを予期せず再起動させ、DoS状態を引き起こす可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: CSCwu51451
CVE ID：CVE-2026-20197
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-2026-76489：複数のシスコ製品におけるSnort 3の汎用ファイル処理メモリ枯渇に関するDoS脆弱性

Snort 3のメモリ管理実装における脆弱性により、複数のシスコ製品が影響を受けます。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ります。

この脆弱性は、Snort 3がファイルを処理する際のエラーチェックが不完全なことに起因し、これにより解放されないメモリが発生する可能性があります。攻撃者は、大量のファイルを送信して処理することで、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検出エンジンを予期せず再起動させ、DoS状態を引き起こす可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: CSCwr25134
CVE ID：CVE-2026-76489
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。

修正リリース

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。

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。

オープンソースの Snort 3

発行時点では、次の表に示すリリース情報は正確でした。

左の列にはSnort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ます。

Snort 3リリース	第 1 修正済みリリース
3.x	3.12.4.0

注：この修正は、セキュリティアドバイザリ『複数のCisco製品Snort 3セキュリティ強化リリース：2026年10月』で公開されている広範な強化機能の一部としても含まれています。

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。

その他のリソース

最適なCisco Secure FTDソフトウェアリリースの判別に関するサポートについては、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新しいリリースが推奨される場合、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 Threat Defense 互換性ガイド

Cisco IOS XEソフトウェアのUTD

発行時点では、次の表に示すリリース情報は正確でした。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。

次の表では、左の列にCisco IOS XEソフトウェアリリースを示します。右の列は、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を示します。

次のUTD Cisco IOS XEソフトウェアイメージには、オープンソースのSnort 3バージョン3.12.4.0が含まれています。

Cisco IOS XE ソフトウェア リリース	第 1 修正済みリリース
17.12	17.12.8(secapp-utd.17.12.08.1.2.8_SV3.12.4.0_XE17.12)
17.15	17.15.6(secapp-utd.17.15.06.1.0.21_SV3.12.4.0_XE17.15)

Cisco IOS XE ソフトウェア リリース	第 1 修正済みリリース
17.18	17.18.5
26.1	26.1.2(secapp-utd.26.01.02.1.0.6_SV3.12.4.0_XE26.1)
26.2	26.2.1

Cisco 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、Cisco Merakiダッシュボードによっ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。Cisco MerakiファームウェアまたはCisco 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10月21日の時点で、このアドバイザリに記載されているモデルのうち、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Cisco Merakiモデルが Snort 3パッケージで自動的に更新されました。

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。

送信元

シスコは、これらの脆弱性を報告していただいた次の方々に感謝いたします。

- Michael BommaritoとClaude AIの協力：CVE-2026-20019、CVE-2026-20179、CVE-2026-20197、CVE-2026-76489
- Talence Security社Tristan Madani氏：CVE-2026-20197
- セキュリティ研究者ヤズダン・ソルター二：CVE-2026-20019

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-misc-dos-6mB22qAK

改訂履歴

バージョン	説明	セクション	Status	日付
1.1	Cisco IOS XEソフトウェアの修正済みリリースに関するUTDの表を更新。	修正リリース	Final	2026年10月22日
1.0	初版リリース	—	Final	2026年10月21日

利用規約

ソフトウェアのダウンロードおよびテクニカルサポート

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。お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定再販業者やシスコ認定パートナーを通じて調達されたもので、ライセンスが有効なものに限ります。

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 Technical Assistance Center（TAC）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。

ソフトウェアのアップグレードを検討する際には、関連す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アップグレード ソリューション一式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。

利用規約の詳細

シスコは、商品適格性または特定目的への適合性に関する保証を含め、明示的か黙示的かを問わず、いかなる種類の保証も表明しません。前述の一般論に限定されることなく、シスコは、本情報の正確性または完全性を保証するものではありません。コンテンツは「現状のまま」提供されます。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。

本セキュリティアドバイザリに含まれる情報のコピーや要約には、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。本セキュリティアドバイザリの最新版については、シスコ セキュリティ アドバイザリ ページをご覧ください。Cisco 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評価します。詳細については、シスコのセキュリティ脆弱性ポリシーを参照してください。

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。