

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



Advisory ID : cisco-sa-hardening-snort3-

ybgmhTQe

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：[9.0](#)

回避策：No workarounds available

Cisco Bug ID：

[CVE-2026-](#)

[20291](#)

[CVE-2026-](#)

[20356](#)

[CVE-2026-](#)

[20236](#)

[CVE-2026-](#)

[20043](#)

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

予防的なセキュリティと製品の品質に対するシスコの継続的な取り組みの一環として、シスコ所有のオープンソースSnort 3ソフトウェアエンジニアリングチームは、包括的な社内セキュリティレビューを実施しました。このレビューの結果、社内で見出された複数の脆弱性に対処するソフトウェアのセキュリティ強化リリースが公開されました。

CVE-2026-20043によって追跡される脆弱性は、Common Weakness Enumeration(CWE)Base CWE-787の下にグループ化された範囲外の書き込みに関する問題に関連しています。

予防的なセキュリティと製品の品質に対するシスコの継続的な取り組みの一環として、シスコ所有のオープンソースSnort 3エンジニアリングチームは、包括的な社内セキュリティレビューを実施しました。このレビューの結果、社内で見出された複数の脆弱性に対処するソフトウェアのセキュリティ強化リリースが公開されました。

これらの脆弱性は内部テストで見出されたものであり、現時点でエクスプロイトの事例は確認されていません。パッチの適用を支援し、開示プロセスを合理化するために、シスコでは、これらの問題を基盤となる脆弱性クラス(Common Weakness Enumeration(CWE))別にグループ化し、各CWEグループに1つのCommon Vulnerabilities and Exposures Identifier(CVE ID)を割り当てました。

注：シスコは、本リリースで対処される個々の脆弱性に関する追加詳細情報を提供するセキュリティアドバイザリを個別に公開することができます。

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-hardening-snort3-ybgmhTQe>

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。

該当製品

脆弱性のある製品

これらの脆弱性は、デバイスの設定に関係なく、次の製品に影響を与えます。

- シスコのクラウド配信ファイアウォール(CDFW)
- Cisco Cyber Vision
- Cisco Meraki MXセキュリティアプライアンス
- シスコセキュアアクセス(CSA)
- Cisco Secure Firewall Threat Defense(FTD)ソフトウェア
- オープンソースの Snort 3
- Cisco IOS XEソフトウェアのUnified Threat Defense(UTD)

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、これらの脆弱性がオープンソースのSnort 2には影響を与えないことを確認しました。

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

次の表に、この強化リリースで対処されている脆弱性クラスの概要を示します。各 CVE ID に割り当てられる CVSS スコアは、その特定の CWE カテゴリ内で最も影響の大きい 1 つの根本的な脆弱性がもたらす可能性がある最大のシビラティ（重大度）を表しています。

CVE ID	CVSS最高スコア	脆弱性クラス (最高レベルのCWE)	説明
CVE-2026-20236	9.0	CWE-682	不正確な計算
CVE-2026-20043	9.0	CWE-787	範囲外の書き込み
CVE-2026-20291	7.8	CWE-269	不適切な権限管理
CVE-2026-20356	7.5	CWE-400	リソース消費の制御なし

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

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

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。

Snort 3リリース	第 1 修正済みリリース
3.x	3.12.4.0

Cyber Vision

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。右の列は、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最初のリリースを示しています。このセクションの表に記載されている適切な[修正済みソフトウェアリリース](#)にアップグレードすることをお勧めします。

Cisco Cyber Visionリリース	第 1 修正済みリリース
5.6 よりも前	修正済みリリースに移行。
5.6	5.6.0

CDFWとCSA

Snort 3は、Snort 3侵入防御システム(IPS)テクノロジーの一部としてCisco CDFWおよびCSAにネイティブに統合され、トラフィックの検査と脅威のブロックを行います。お客様のアクションは必要ありません。2026年10月21日の時点で、すべてのCisco CDFWおよびCSAクラウドインスタンスがSnort 3パッケージで自動的に更新されています。

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MerakiモデルがSnort 3パッケージで自動的に更新されました。

Cisco Secure FTD ソフトウェア

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。右の列は、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最初のリリースを示しています。このセクションの表に記載されている適切な[修正済みソフトウェアリリース](#)にアップグレードすることをお勧めします。

Cisco Secure FTD ソフトウェアリリース	第 1 修正済みリリース
7.0 以前	7.0.10
7.2	7.2.12
7.4	7.4.8
7.6	7.6.6
7.7	7.7.13
10.0	10.0.2
10.1	10.1.0

Cisco IOS XEソフトウェアのUTD

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。右の列は、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最初のリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

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)
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

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

これらの脆弱性は、既存のテストプロセスおよびフロンティアの AI モデルを使用した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-hardening-snort3-ybgmhTQe>

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。