シスコ製品に影響するNode.jsおよびBrotliの脆弱性：2026年10月

High

Advisory ID : cisco-sa-oct2026-node-js-Jj3SQ19u
初公開日 : 2026-10-27 21:30
注: : 2026-11-04 18:52
バージョン 1.5 : Interim
回避策 : No workarounds available
Cisco Bug ID :

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

2026年10月21日、Node.jsは、22.x、24.x、および26.xのサポートされているリリース行において、複数の脆弱性に対する修正が利用可能であることを発表しました。

これらの脆弱性は、Brotliデコーダ、DNS解決、TLS証明書の検証などの重要な操作に影響を与えます。この脆弱性は、リモートコード実行とトラフィック代行受信にリスクをもたらします。詳細については、「Node.jsセキュリティリリース」を参照してください。

次の脆弱性のセキュリティ影響評価(SIR)は高く、このアドバイザリで説明されています。

- CVE-2026-111497:Brotliデコーダの範囲外の書き込み。リモートでコードが実行される可能性がある
- CVE-2026-105482：埋め込みNUL文字が含まれるDNS解決のトランケート
- CVE-2026-105483：全角IPディジットを使用したTLSホスト名検証バイパス
- CVE-2026-106069:TLSホスト名検証バイパス（非正規IPアドレス使用）

Splunk製品および製品の詳細については、Splunk製品のNode.js(CVE-2026-111497、CVE-2026-105482、CVE-2026-105483、CVE-2026-106069)の脆弱性（2026年10月）を参照してください

この調査は、2026年10月30日にNode.jsの外部のBrotliをカバーするように拡張されました。Google Brotli Cデコーダに含まれるBrotliデコーダの欠陥(CVE-2026-111497)は、他のソフトウェアにバンドルまたはリンクされていることが多いため、Node.jsを超える製品が影響を受ける可能性があります。該当するソフトウェアについては、ブロッコリー2シェルを参照してください。

重要：製品がこのアドバイザリに記載されていない場合、シスコのレビューによると、その製品はこの脆弱性の影響を受けません。

このアドバイザリは、追加の情報が入手可能になり次第、更新されます。

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-oct2026-node-js-Jj3SQ19u

該当製品

シスコでは、これらの脆弱性の影響を受ける製品を判断するために、製品ラインを調査中です。調査の進捗に応じて、シスコはこのアドバイザリを更新し、影響を受ける製品に関する情報を提供します。

「脆弱性のある製品」のセクションで、影響を受ける各製品の Cisco Bug ID を示します。バグはCisco Bug Search Toolで検索できるようになっており、回避策（利用可能な場合）と修正されたソフトウェアリリースなど、プラットフォーム固有の追加情報が記載されます。

シスコの優先製品のステータス

次の表に、シスコの優先製品と、本アドバイザリに記載された脆弱性の影響に対する調査の状況を示します。

シスコ製品	Status
Catalyst SD-WANソフトウェア	影響なし
Identity Services Engine（ISE）	影響なし
IOS ソフトウェア	調査中
IOS XE ソフトウェア	調査中
IOS XR ソフトウェア	調査中
NX-OS ソフトウェア	調査中
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	調査中
Cisco Secure Firewall Management Center（FMC）ソフトウェア	調査中
セキュアファイアウォール脅威対策(FTD)	影響なし

重要：製品がこのアドバイザリに記載されていない場合、シスコのレビューによると、その製品はこの脆弱性の影響を受けません。

その他調査中の製品

また、本アドバイザリに記載された脆弱性の影響に関して以下の製品についても現在調査中です。

アプリケーションの監視

AppDynamics
AppDynamicsエンタープライズコンソール
AppDynamics仮想アプライアンス
ケーブルデバイス
インテリジェント ノード マネージャ
コラボレーションとソーシャルメディア
コラボレーション用AI POD
ネットワークおよびコンテンツ セキュリティ デバイス
暗号化サービスPureCA（プライベートPKI CA）
ハイパーシールド
セキュアファイアウォール適応型セキュリティ仮想アプライアンス(ASAv)
Secure IPS(旧称：Cisco Next-Generation Intrusion Prevention System(NGIPS))
ネットワーク管理とプロビジョニング
BGPトラフィックエンジニアリングコントローラ
Crosswork Hierarchical Controller
Crosswork Workflow Manager
Elastic Services Controller(ESC)
オプティカル ネットワーク コントローラ
Optical Network Planner
Provider Connectivity Assurance
Routing and Switching - Enterprise and Service Provider
ASR 5000シリーズソフトウェア(StarOS)
クラウドネイティブ導入プラットフォーム(CNDP)
エンタープライズ NFV インフラストラクチャ ソフトウェア（NFVIS）
NextFusionプラットフォーム
ポリシースイート(CPS)
Ultra Packet Core - Redundancy Configuration Manager(RCM)
ユニファイド コンピューティング
HyperFlex HX Data Platform
ビデオ、ストリーミング、テレプレゼンス、およびトランスコーディングデバイス
Webexデスクカメラ
音声およびユニファイド コミュニケーション デバイス
Cloud Connect
ワイヤレス

コネクテッドモバイルエクスペリエンス(CMX)
産業用ワイヤレスモニタ
シスコクラウドホステッドサービス
Cloud Native Application Observability
Cloudlock
IoT Operations Dashboard
LMA
堅牢なインテリジェンスRIME
Cisco Secure Workload SaaS
セキュリティクラウドサインオン
Smartlook
ThousandEyes
Vidcast
脆弱性管理（以前のKenna.VM）
Webex AIエージェント
会議用WebEx Assistant
Webexコラボレーションコントロールハブ
Webex Contact Center
Webex統合とボット
Webexインタラクション
Cisco のサービス
ビジネスクリティカルな洞察
CDT
CX Cloud
知能指数
マネージドサービスプラットフォーム
クラウドの準備評価ツール

重要：製品がこのアドバイザリに記載されていない場合、シスコのレビューによると、その製品はこの脆弱性の影響を受けません。

脆弱性のある製品

シスコの優先製品に対するこれらの脆弱性の影響に関する調査状況については、「シスコの優先製品の状況」の項を参照してください。

シスコでは、これらの脆弱性の影響を受ける製品と影響の範囲を特定するために、製品ラインを調査中です。このセクションは、情報が入手可能になった時点で更新されます。

影響を受ける製品とソフトウェア修正

シスコ製品	Cisco Bug ID	修正済みリリースが利用可能
ケーブルデバイス		
Smart PHY	CSCwx49006	リリース番号未定（2027年3月）
エンドポイントクライアントとソフトウェア		
パケット トレーサ		9.2.0（2026年12月）
ネットワークおよびコンテンツ セキュリティ デバイス		
Duoネットワークゲートウェイ		3.4.2
Windows用Duo Authentication Proxy Local Manager		6.8.1 （2026年11月）
Cisco Secure Workload		リリース番号今後、定義予定。
ネットワーク管理とプロビジョニング		
ビジネスプロセスの自動化(BPA)	CSCwx48997	4.1.2（未定） 5.0（2026年11月） 5.1（未定）
Catalyst Center（旧DNA Center）	CSCwx48988	3.4.1（2027年7月）
マルチサイトオーケストレータ		2027.1.0 （2026年11月）
セキュアエンドポイント – プライベートクラウドアプライアンス	CSCwx48980	リリース番号未定（2026 年 11 月）
仮想インフラストラクチャ マネージャ	CSCwx48998	リリース番号今後、定義予定。
Routing and Switching - Enterprise and Service Provider		
プライベート5G	CSCwx48976	22.23.4（未定）
ユニファイド コンピューティング		
Intersight 仮想アプライアンス		リリース番号未定（2026 年 11 月）
シスコクラウドホステッドサービス		
AIキャンバス		リリース番号今後、定義予定。
AppDynamics SaaS		リリース番号今後、定義予定。
セキュリティクラウド制御		20261030-b3cffcb （2026年11月）
Intersight		リリース番号未定（2026 年 11 月）
Spaces		24.22.1
Webex Connect		6.22.2 （2026年11月）

シスコ製品	Cisco Bug ID	修正済みリリースが利用可能
Cisco のサービス		
CLI アナライザ		リリース番号今後、定義予定。

重要：製品がこのアドバイザリに記載されていない場合、シスコのレビューによると、その製品はこれらの脆弱性の影響を受けません。

脆弱性を含んでいないことが確認された製品

シスコの優先製品に対するこれらの脆弱性の影響に関する調査状況については、「シスコの優先製品の状況」の項を参照してください。

シスコは、この問題が以下のシスコ製品には影響を与えないことを確認しました。

エンドポイント クライアントとクライアント ソフトウェア
Secure Client（旧称AnyConnect Secure Mobility Client）
ネットワークおよびコンテンツ セキュリティ デバイス
ISEパッシブIDコネクタ(ISE-PIC)
セキュアマルウェア分析 – プライベートクラウド（アプライアンス）
Cisco Secure Network Analytics
Telemetry Broker
ネットワーク管理とプロビジョニング
Business ダッシュボード
Catalyst SD-WAN分析
Catalyst SD-WANコントローラ
Catalyst SD-WANポータル
Catalyst SD-WAN Manager
Catalyst SD-WANバリデータ
Data Center Network Manager
ライセンス(Smart Software Manager)オンプレミス
メッシュポリシーエンジン
Nexus Dashboard
SANインサイトの検出
ThousandEyes Enterprise エージェント
ThousandEyes Enterprise Agent：シスコアプリケーションホスティング
Routing and Switching - Enterprise and Service Provider
Ultra Cloud Core：サブスクライバ マイクロサービス インフラストラクチャ

シスコクラウドホステッドサービス
Duo
IoT Control Center
セキュアなアクセス
セキュアなEメールクラウドゲートウェイ
Cisco Secure Email Threat Defense
包括CDaaS
WG2
Cisco のサービス
セキュア転送サービス
Merakiデバイス
Meraki ダッシュボード
Meraki MRシリーズデバイス
Meraki MSシリーズデバイス
Meraki MXシリーズデバイス
ユニファイド コンピューティング
UCSソフトウェア
UCS Manager ソフトウェア

重要：製品がこのアドバイザリに記載されていない場合、シスコのレビューによると、その製品はこの脆弱性の影響を受けません。

回避策

すべての回避策は、製品固有のCisco Bugとして文書化され、それぞれこのアドバイザリの「脆弱性のある製品」セクションで特定されます。

修正済みソフトウェア

修正済みソフトウェアリリースの詳細については、このアドバイザリの「脆弱性が存在する製品」セクションに記載されているCisco Bug IDを参照してください。

ソフトウェアのアップグレードを検討する際は、Cisco Security Advisories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。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、このアドバイザリで説明されている脆弱性に対して概念実証段階のエクスプロイトコードが入手可能であることを認識しています。

Cisco PSIRTでは、Cisco製品に対するこれらの脆弱性の不正利用事例は確認しておりません。

送信元

これらの脆弱性はNode.jsによって公開されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-oct2026-node-js-Jj3SQ19u

改訂履歴

バージョン	説明	セクション	Status	日付
1.5	タイトル、概要、脆弱性のある製品、脆弱性を含んでいないことが確認された製品を更新。	タイトル、概要、該当製品	暫定	2026年11月4日
1.4	「脆弱性のある製品」と「脆弱性が存在しないことが確認された製品」を更新。	該当製品	暫定	2026年11月2日
1.3	「脆弱性のある製品」と「脆弱性が存在しないことが確認された製品」を更新。	該当製品	暫定	2026年10月30日
1.2	「脆弱性のある製品」と「脆弱性が存在しないことが確認された製品」を更新。	該当製品	暫定	2026年10月29日
1.1	「脆弱性のある製品」と「脆弱性が存在しないことが確認された製品」を更新。Splunkアドバイザリへのリンクを追加。	概要および該当製品	暫定	2026年10月28日
1.0	初版リリース	—	暫定	2026年10月27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。