Erlang/OTP SSH サーバーにおける複数のシスコ製品の認証されていないリモートコード実行：2025 年 4 月

アドバイザリーID : cisco-sa-erlang-otp-ssh-xyZZy
CVE-2025-32433
初公開日 : 2025-04-22 21:45
最終更新日 : 2025-06-11 14:40
バージョン 1.11 : Final
CVSSスコア : 10.0
回避策 : No workarounds available
Cisco バグ ID :

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

2025 年 4 月 16 日に、Erlang/OTP SSH サーバーの重大な脆弱性が公開されました。この脆弱性により、認証されていないリモートの攻撃者が該当デバイスでリモートコード実行（RCE）を行う可能性があります。

この脆弱性は、認証フェーズにおける SSH メッセージの処理の不具合に起因します。

この脆弱性の説明については、Erlang の発表を参照してください。

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-erlang-otp-ssh-xyZZy

該当製品

シスコでは、この脆弱性の影響を受ける可能性がある製品を判断するために、Erlang/OTP を含む製品ラインを調査しました。

このアドバイザリには、影響を受けるソフトウェアコンポーネントが含まれていることが確認されているため、脆弱性が存在する可能性のあるシスコの製品とサービスのみが記載されています。影響を受けるソフトウェアコンポーネントを含まない製品およびサービスは脆弱ではないため、このアドバイザリには記載されていません。このアドバイザリの「影響を受ける製品」セクションに明示的に記載されていないシスコ製品またはサービスは、記載されている脆弱性の影響を

受けません。

「脆弱性が存在する製品」の項には、影響を受ける製品の Cisco Bug ID を示します。Cisco Bug は Cisco Bug Search Tool で検索可能であり、回避策（使用可能な場合）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。

脆弱性のある製品

次の表に、本アドバイザリに記載された脆弱性の影響を受けるシスコ製品を示します。将来のソフトウェア リリース日が示されている場合、その日付はこのアドバイザリの上部にある最終更新日時点でシスコが把握しているすべての情報に基づいた日付になります。このソフトウェア リリースの日付は、試験結果や優先される機能や修正の提供等いくつかの理由により変更される場合があります。詳細については、関連するシスコのバグを参照してください。

シスコ製品	Cisco Bug ID	修正済みリリースが利用可能
ネットワーク アプリケーション、サービス、およびアクセラレーション		
ConfD、ConfD Basic[1]	CSCwo83759	7.7.19.1 8.0.17.1 8.1.16.2 8.2.11.1 8.3.8.1 8.4.4.1
ネットワーク管理とプロビジョニング		
Network Services Orchestrator（NSO）[1]	CSCwo83796	5.7.19.1 6.1.16.2 6.2.11.1 6.3.8.1 6.4.1.1 6.4.4.1
Smart PHY[1]	CSCwo83751	25.2（2025年9月）
Ultra Services Platform[1]	CSCwo83750	修正予定はありません。
Routing and Switching - Enterprise and Service Provider		
ASR 5000 シリーズ ソフトウェア（StarOS）、Ultra Packet Core[1]	CSCwo83806	2025.03（2025年7月）
Cloud Native Broadband Network Gateway[1]	CSCwo83769	2025.03.1（2025 年 8 月）
iNode Manager	CSCwo83755	修正の予定はありません。[2]

シスコ製品	Cisco Bug ID	修正済みリリースが利用可能
Optical Site Manager for Network Convergence System（NCS）1000 シリーズ[1]	CSCwo83800	25.2.1（2025 年 6 月） 25.3.1（2025 年 9 月）
NCS 2000 シリーズのシェルフ仮想化オーケストレータモジュール[1]	CSCwo83774	25.1.1 （2025年6月）
Ultra Cloud Core：アクセスおよびモビリティ管理機能[1]	CSCwo83785	2025.03.1（2025 年 8 月）
Ultra Cloud Core：ポリシー制御機能[1]	CSCwo83789	2025.03.1（2025 年 8 月）
Ultra Cloud Core：Redundancy Configuration Manager[1]	CSCwo83753	2025.03.1（2025 年 8 月）
Ultra Cloud Core：セッション管理機能[1]	CSCwo83775	2025.03.1（2025 年 8 月）
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[1]	CSCwo83747	2025.03.1（2025 年 8 月）
Unified Computing		
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）[1]	CSCwo83758	4.18（2025年8月）
ルーティングおよびスイッチング - スモール ビジネス		
Small Business RV シリーズ ルータ RV160、RV160W、RV260、RV260P、RV260W、RV340、RV340W、RV345、RV345P	CSCwo83803 CSCwo83767	修正の予定はありません。[3]

1. これらの製品は、認証されていないチャネル要求メッセージを受け入れるため脆弱ですが、製品の構成により、RCE に対しては脆弱ではありません。
2. iNode Manager は、ソフトウェアメンテナンスが終了しました。 Cisco iNode Manager およびインテリジェント ノード ローカル制御ソフトウェアの販売終了およびサポート終了のお知らせ。
3. これらのルータは、ソフトウェアメンテナンスが終了しました。 Cisco RV 160、RV260、RV345P、RV340W、RV260W、RV260P、および RV160W VPN ルータの販売終了およびサポート終了のお知らせ。

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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性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。

ネットワークおよびコンテンツ セキュリティ デバイス
FXOS ソフトウェア
Identity Services Engine（ISE）
Cisco Secure Adaptive Security Appliance（ASA）ソフトウェア
Cisco Secure Firewall Management Center（FMC）ソフトウェア
Cisco Secure Firewall Threat Defense（FTD）ソフトウェア
Secure Network Analytics（SNA）
ネットワーク アプリケーション、サービス、およびアクセラレーション
自動障害管理
Wide Area Application Services（WAAS）Software
ネットワーク管理とプロビジョニング
Application Policy Infrastructure Controller（APIC）
Crosswork Hierarchical Controller
Cyber Vision
Elastic Services Controller
Evolved Programmable Network Manager（EPNM）
FindIT ネットワーク管理ソフトウェア
Policy Suite
Provider Connectivity Assurance
Virtual Topology System
仮想インフラストラクチャ マネージャ
WAE の自動化
Routing and Switching - Enterprise and Service Provider
Catalyst Center
Catalyst SD-WAN Manager
Catalyst SD-WAN
Intelligent Node ソフトウェア
IOS ソフトウェア
IOS XE ソフトウェア
IOS XR ソフトウェア
Meraki 製品
NX-OS ソフトウェア

ルーティングおよびスイッチング - スモール ビジネス
Business ダッシュボード
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
Expressway および TelePresence Video Communication Server（VCS）

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、本アドバイザリの「脆弱性のある製品」セクションに記載されている 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には、シスコ セキュリティ アドバイザリ 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

2025年6月、Cisco Product Security Incident Response Team(PSIRT)は、この脆弱性の不正利用が試みられたことを認識しました。これらの脆弱性が修正済みのソフトウェアリリースにアップグレードすることを、引き続き強くお勧めします。

出典

この脆弱性は、Erlang/OTP Github Issues Tracker を通じて公に報告されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-erlang-otp-ssh-xyZZy

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.11	CISA KEVに追加された脆弱性	不正利用事例と公式発表	Final	2025年6月11日
1.10	製品リストとステータスを更新。アドバイザリのステータスを[Final]に変更。	ヘッダーと脆弱な製品	Final	2025年6月10日
1.9	製品リストとステータスを更新。	脆弱性が存在する製品	Interim	2025年5月30日
1.8	製品リストとステータスを更新。	脆弱性が存在する製品	Interim	2025年5月28日
1.7	製品リストとステータスを更新。	脆弱性が存在する製品	Interim	2025 年 5 月 7 日
1.6	製品リストとステータスを更新。	脆弱性が存在する製品	Interim	2025 年 4 月 30 日
1.5	製品リストとステータスを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含んでいないことが確認された製品	Interim	2025 年 4 月 29 日
1.4	製品リストとステータスを更新。	脆弱性が存在する製品	Interim	2025 年 4 月 28 日
1.3	製品リストとステータスを更新。	「調査中の製品」、「脆弱性が存在する製品」、「脆弱性が存在しない製品」	Interim	2025 年 4 月 25 日
1.2	製品リストとステータスを更新。	「調査中の製品」、「脆弱性が存在する製品」、「脆弱性が存在しない製品」	Interim	2025 年 4 月 24 日
1.1	製品リストとステータスを更新。	「調査中の製品」、「脆弱性が存在する製品」、「脆弱性が存在しない製品」	Interim	2025 年 4 月 23 日
1.0	初回公開リリース	—	Interim	2025 年 4 月 22 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。