# OpenSSHサーバにおけるリモート非認証コード実行の脆弱性(regreSSHion):2024年7月

High

アドバイザリーID : cisco-sa-openssh-rce-2024
初公開日 : 2024-07-02 16:00
最終更新日 : 2024-07-12 15:48
バージョン 1.8 : Interim
CVSSスコア : 8.1
回避策 : No workarounds available
Cisco バグ ID :

CVE-2024-6387

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

2024年7月1日、Qualys Threat Research Unit(TRU)は、glibcベースのLinuxシステムのOpenSSHサーバ(sshd)に影響を与える、認証されていないリモートコード実行の脆弱性を公開しました。

CVE-2024-6387: sshdでシグナルハンドラの競合状態が見つかりました。クライアントはLoginGraceTime秒以内に認証を受けません（デフォルトは120、古いOpenSSHバージョンでは600）。その後、sshd SIGALRMハンドラが非同期で呼び出されます。ただし、このシグナルハンドラは非同期シグナルセーフでない様々な関数、例えばsyslog()をコールします。

この脆弱性の詳細については、Qualysセキュリティアドバイザリを参照してください。

このアドバイザリは追加情報が入手可能になった時点で更新されます。

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-openssh-rce-2024

## 該当製品

シスコでは、この脆弱性の影響を受ける製品およびクラウド サービスを判断するために、製品ラインを調査中です。調査の進行に伴い、シスコはこのアドバイザリを更新し、影響を受ける製品およびサービスについてお知らせします。

「脆弱性のある製品」のセクションで、影響を受ける各製品またはサービスの 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。

## 調査中の製品

現在、この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シスコ製品を調査中です。

ネットワーク管理とプロビジョニング

- Application Policy Infrastructure Controller（APIC）
- Nexus Dashboard,（旧称：Application Services Engine）

Unified Computing

- Integrated Management Controller（IMC）Supervisor
- UCS マネージャ

### 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。影響を受けるコンポーネントについてバージョン情報や日付がリストに記載されていない場合（空欄や暫定とされているもの）、シスコは修正の評価を続けており、追加情報が確認された時点でアドバイザリを更新します。アドバイザリがFinalとマークされた後に詳細を確認するには、関連するCisco Bugsを参照してください。

| 製品 | Cisco Bug ID | Fixed Release Availability |
|---|---|---|
| ネットワークおよびコンテンツ セキュリティ デバイス | | |
| 適応型セキュリティ アプライアンス（ASA）ソフトウェア | CSCwk62296 | |
| Firepower 4100/9300 FXOS Firepowerシャーシマネージャ | CSCwk62297 | 2.12.1（2024年7月） |
| Firepower Management Center（FMC）ソフトウェア | CSCwk62296 | |
| Firepower Threat Defense（FTD）ソフトウェア | CSCwk62296 | |
| Identity Services Engine（ISE） | CSCwk61938 | 3.3パッチ（2024年7月）<br>3.2パッチ（2024年9月 |

| | | |
|---|---|---|
| | | ）<br>3.1パッチ（2024年7月）） |
| セキュアアクセスリソースコネクタ | CSCwk67866 | 2.0.0-2407032046（2024年7月） |
| Cisco Secure Email and Web Manager | CSCwk63532 | 15.5.2 MR（2024年8月） |
| セキュアEメールゲートウェイ | CSCwk63523 | 15.5.2 MR（2024年8月）<br>15.0.3 MR（2024年11月）<br>16.0 (Oct 2024) |
| Cisco Secure Network Analytics | CSCwk62315 | 7.4.2（2024年7月）<br>7.5.0（2024年7月） |
| ネットワーク管理とプロビジョニング | | |
| Common Services Platform Collector（CSPC） | CSCwk62250 | 2.11.0.1（2024年7月） |
| Crosswork Data Gateway | CSCwk62311 | 7.0.0（2024年8月） |
| Cyber Vision | CSCwk62289 | 4.1.7（2024年7月）<br>4.4.3（2024年7月）<br>5.0.0（2024年7月） |
| Cisco DNA Spaces コネクタ | CSCwk62273 | コネクタ3（2024年7月） |
| Evolved Programmable Network Manager(EPNM) | CSCwk62268 | |
| Prime Collaboration Deployment | CSCwk64755 | 15.0.1.12900（2024年9月）<br>15SU2（2024年9月） |
| Prime インフラストラクチャ | CSCwk62276 | 3.10.5（2024年7月） |
| Smart PHY | CSCwk62284 | 24.2（2024年9月） |
| Smart Software Manager オンプレミス | CSCwk62288 | |
| 仮想インフラストラクチャ マネージャ | CSCwk62277 | 5.0.1（2024年8月） |
| Routing and Switching - Enterprise and Service Provider | | |
| 8000 シリーズ ルータ | CSCwk62108 | |
| ASR 5000 シリーズ ルータ | CSCwk62248 | |
| Catalyst ESS9300エンベデッドシリーズスイッチ | CSCwk67488 | 17.15（2024年7月） |
| Catalyst IE3x00高耐久性シリーズスイッチ | CSCwk67488 | 17.15（2024年7月） |
| Catalyst IE 9300高耐久性シリーズスイッチ | CSCwk67488 | 17.15（2024年7月） |

| | | |
|---|---|---|
| エンベデッドサービス 3300 シリーズ スイッチ | CSCwk67488 | 17.15（2024年7月） |
| GGSN Gateway GPRS Support Node | CSCwk62248 | |
| NETCONFが有効なIOS XEソフトウェア | CSCwk61216 | |
| IOS XRd コントロールプレーン | CSCwk62108 | |
| IOS XRd vRouters | CSCwk62108 | |
| IP Services Gateway（IPSG） | CSCwk62248 | |
| MDS 9000 シリーズ マルチレイヤ スイッチ | CSCwk62258 | |
| MME モビリティ マネジメント エンティティ | CSCwk62248 | |
| NCS540Lイメージを実行するNetwork Convergence System 540シリーズルータ | CSCwk62108 | |
| Network Convergence System 1010 | CSCwk62108 | |
| Network Convergence System 1014 | CSCwk62108 | |
| Network Convergence System 5700固定シャーシNCS-57B1、NCS-57C1、およびNCS-57D2 | CSCwk62108 | |
| Nexus 3000 シリーズ スイッチ | CSCwk61235 | 10.2.x（2025年1月）<br>10.3.x（2024年8月）<br>10.4.x（2024年10月）<br>10.5.x（2024年8月） |
| ACI モードの Nexus 9000 シリーズ ファブリック スイッチ | CSCwk62257 | |
| スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ | CSCwk61235 | 10.2.x（2025年1月）<br>10.3.x（2024年8月）<br>10.4.x（2024年10月）<br>10.5.x（2024年8月） |
| PDSN/HA Packet Data Serving Node and Home Agent | CSCwk62248 | |
| PGW Packet Data Network Gateway | CSCwk62248 | |
| System Architecture Evolution(SAE)ゲートウェイ | CSCwk62248 | |
| Ultra Cloud Core：セッション管理機能 | CSCwk62246 | |
| 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 | CSCwk62247 | 2024.03.1（2024年7月） |
| Ultra Cloud Core 5Gポリシー制御機能 | CSCwk62244 | |
| Ultra Packet Core | CSCwk62248 | |
| Unified Computing | | |
| Intersight 仮想アプライアンス | CSCwk63145 | 1.0.9-677 |
| UCS C シリーズ ラックサーバーおよび S シリーズ | CSCwk62266 | 4.3.4（2024年8月） |

| | | |
|---|---|---|
| ストレージサーバー - Integrated Management Controller（CIMC） | | 4.3.2（2024年8月） |
| UCS Director | CSCwk62255 | 6.9.1.0（2024年10月） |
| 音声およびユニファイド コミュニケーション デバイス | | |
| デスク電話9841 | CSCwk62323 | 3.2(1)（2024年10月） |
| デスク電話9851 | CSCwk62323 | 3.2(1)（2024年10月） |
| Emergency Responder | CSCwk63694 | 15.0.1.12900（2024年9月）<br>15SU2（2024年9月） |
| Unified Communications Manager/Unified Communications Manager Session Management Edition | CSCwk62318 | 15.0.1.12900（2024年9月）<br>15SU2（2024年9月） |
| Unified Communications Manager IM and Presence Service | CSCwk63634 | 15.0.1.12900（2024年9月）<br>15SU2（2024年9月） |
| Unified Contact Center Express（Unified CCX） | CSCwk62320 | |
| Unity Connection | CSCwk63494 | |
| Video Phone 8875 | CSCwk62317 | 2.3(1) (Nov 2024) |
| 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 | | |
| Board シリーズ | CSCwk70371 | RoomOS 11.18.1.6 |
| Cisco Meeting Server | CSCwk62286 | SMU - CMS 3.9.2（2024年8月）<br>SMU - CMS 3.8.2（2024年8月） |
| Desk シリーズ | CSCwk70371 | RoomOS 11.18.1.6 |
| Expressway シリーズ | CSCwk61630 | X15.0.3（2024年7月）<br>X15.2.0（2024年9月） |
| Room シリーズ | CSCwk70371 | RoomOS 11.18.1.6 |
| TelePresence Video Communication Server（VCS） | CSCwk61630 | X15.0.3（2024年7月）<br>X15.2.0（2024年9月） |
| Webex Board | CSCwk70371 | RoomOS 11.18.1.6 |
| Webex DX80 | CSCwk70371 | RoomOS 11.18.1.6 |
| ワイヤレス | | |
| 6300シリーズエンベデッドサービスアクセスポイン | CSCwk62269 | 17.15（2024年7月） |

| | | |
|---|---|---|
| ト | | 17.9.6（2024年8月）<br>17.12.4（2024年7月） |
| Aironet 802.11ac Wave2アクセスポイント | CSCwk62269 | 17.15（2024年7月）<br>17.9.6（2024年8月）<br>17.12.4（2024年7月） |
| Aironet 1540 シリーズ | CSCwk62269 | 17.15（2024年7月）<br>17.9.6（2024年8月）<br>17.12.4（2024年7月） |
| Aironet 1560 シリーズ | CSCwk62269 | 17.15（2024年7月）<br>17.9.6（2024年8月）<br>17.12.4（2024年7月） |
| Catalyst 9100シリーズアクセスポイント | CSCwk62269 | 17.15（2024年7月）<br>17.9.6（2024年8月）<br>17.12.4（2024年7月） |
| Catalyst IW6300ヘビーデューティシリーズアクセスポイント | CSCwk62269 | 17.15（2024年7月）<br>17.9.6（2024年8月）<br>17.12.4（2024年7月） |
| Catalyst IW9165ヘビーデューティシリーズ | CSCwk62269 | 17.15（2024年7月）<br>17.9.6（2024年8月）<br>17.12.4（2024年7月） |
| Catalyst IW9165高耐久性シリーズ | CSCwk62269 | 17.15（2024年7月）<br>17.9.6（2024年8月）<br>17.12.4（2024年7月） |
| Catalyst IW9167ヘビーデューティシリーズ | CSCwk62269 | 17.15（2024年7月）<br>17.9.6（2024年8月）<br>17.12.4（2024年7月） |
| コネクテッド モバイル エクスペリエンス | CSCwk62270 | CMX 11.0.1パッチ（2024年8月） |
| IEC6400エッジコンピューティングアプライアンス | CSCwk62290 | 1.0.2（2024年8月）<br>1.1.0（2024年10月） |

## 脆弱性を含んでいないことが確認された製品

シスコでは、こ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。この項は情報が入手可能になった時点で更新されます。

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。

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

- AnyConnect セキュア モビリティ クライアント

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

- Cloud Services Platform 5000 シリーズ
- 安全なワークロード

ネットワークおよびコンテンツ セキュリティ デバイス

- セキュアエンドポイントプライベートクラウド
- Cisco Secure Web Appliance
- Umbrella 仮想アプライアンス

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
- Catalystセンター
- Catalyst Centerアシュアランス
- Cisco Telemetry Broker
- Crosswork Change Automation
- Crosswork Health Insights
- Crosswork Zero Touch Provisioning（ZTP）
- Modeling Labs
- Network Services Orchestrator（NSO）
- Policy Suite
- Prime Cable Provisioning
- Prime Network Registrar
- SecureXオーケストレーションリモート
- ThousandEyes Enterprise エージェント
- WAN Automation Engine（WAE）

Routing and Switching - Enterprise and Service Provider

- ASR 9000 シリーズ アグリゲーション サービス ルータ
- Industrial Ethernet 1000 シリーズ スイッチ
- Industrial Ethernet 2000 シリーズ スイッチ

- Industrial Ethernet 3000 シリーズ スイッチ
- Industrial Ethernet 4000 シリーズ スイッチ
- Industrial Ethernet 5000 シリーズ スイッチ
- IOS ソフトウェア
- IOS XRv 9000シリーズルータ
- IOS XR 64ビット(eXR)ソフトウェアを実行するNetwork Convergence System 540シリーズルータ
- Network Convergence System 560 シリーズ ルータ
- Network Convergence System 1001
- Network Convergence System 1002
- Network Convergence System 1004
- Network Convergence System 5000 シリーズ ルータ
- Network Convergence System（NCS）5500 シリーズルータ
- IOS XR 64ビット(eXR)ソフトウェアを実行しているNetwork Convergence System 5700シリーズルータ
- Nexus 1000V シリーズ スイッチ
- Nexus 5500 プラットフォーム スイッチ
- Nexus 5600 プラットフォーム スイッチ
- Nexus 6000 シリーズ スイッチ
- Nexus 7000 シリーズ スイッチ
- オプティカル ネットワーク コントローラ

Unified Computing

- Intersightマネージドモード(IMM)のUCSファブリックインターコネクトのデバイスコンソール
- HyperFlex System
- UCS Central Software
- UCS E シリーズ サーバ

音声およびユニファイド コミュニケーション デバイス

- Computer Telephony Integration Object Server（CTIOS）
- Finesse
- Unified Contact Center Enterprise（Unified CCE）
- Unified Contact Center Enterprise – クラウドコネクト
- Unified Customer Voice Portal（Unified CVP）
- Unified Intelligence Center
- Unified Intelligent Contact Management Enterprise

ワイヤレス

- 800および1900シリーズISR統合型アクセスポイント

- AireOSワイヤレスLANコントローラ
- Aironet 700 シリーズ アクセス ポイント
- Aironet 700W シリーズ アクセス ポイント
- Aironet 802.11ac Wave1アクセスポイント産業用ワイヤレス3700シリーズ
- Aironet 1530 シリーズ
- Aironet 1550 シリーズ
- Aironet 1570 シリーズ
- 超高信頼ワイヤレスバックホール

シスコ クラウド ホステッド サービス

- AppDynamics
- 動脈瘤
- 攻撃対象領域の管理
- ビジネスクリティカルなサービス
- シスコマネージドサービスプラットフォーム
- Cisco Secureクライアント
- Cisco University – 次世代ラーニング
- クラウドネイティブアプリケーションの可観測性
- Crossworkクラウド
- カスタマージャーニープラットフォームR10
- データサイエンスサービス
- DevNetクラウドサービス
- DevNetサンドボックス
- eSIM Flex
- Intersight SaaS
- IoTコントロールセンター
- IoT運用ダッシュボード
- Kennaプラットフォーム
- マネージドサービスアクセラレータ(MSXaaS)
- マトリックスネットワークインテリジェンスサービス
- ネットワークプラグアンドプレイ接続
- 可観測性プラットフォーム
- 全視神経
- Provider Connectivity Assurance（旧称：Skylight Performance Analytics）
- Secure Cloud Analytics
- セキュアなEメールクラウド
- Secure Email Encryption Service（旧称Registered Envelope Service）
- セキュアなEメール脅威に対する防御
- Secure Endpoint
- セキュアマルウェア分析
- 安全なワークロードSaaS

- Slido
- スマートな
- スマートソフトウェアマネージャ
- UC管理
- 超高信頼ワイヤレスバックホール
- ユーザ定義ネットワーククラウド
- ビデオキャスト
- Webex Calling
- Webex Contact Center
- Webexイベント
- Webex – 会議 – メッセージングアプリ – 通話
- WebEx Teams
- XDRの

## 詳細

この脆弱性に対するシスコの回答

シスコは、CVE-2024-6387による影響について、すべての製品およびサービスの評価を継続しています。この脆弱性の不正利用を検出するために、シスコは次のSnortルールをリリースしました。

- 33654
- 63659

シスコでは、信頼できるホストだけにSSHアクセスを制限することを推奨しています。SSHサービスへのアクセスを防止するためにインフラストラクチャアクセスコントロールリスト(ACL)を適用する手順については、次のガイドを参照してください。

- Cisco IOSデバイスのセキュリティ強化に関するシスコガイド – インフラストラクチャACLによるネットワークアクセス制限
- NX-OSソフトウェアデバイスの保護に関するシスコのガイド – インフラストラクチャACLによるネットワークアクセス制限
- Cisco UCS強化ガイド – ルータおよびファイアウォールでのACLによるネットワークアクセスの制限
- Ciscoファイアウォールのベストプラクティス – 管理プレーンの保護
- Cisco Firepower Threat Defense強化ガイド

強化に関するその他のドキュメントについては、「戦術的リソース」を参照してください。

## 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。

## 不正利用事例と公式発表

Cisco 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コンセプト実証エクスプロイトコードが利用可能であることを認識しています。ただし、エクスプロイトにはカスタマイズが必要です。

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

## 出典

この脆弱性は、2024年7月1日にQualys Threat Research Unitによって公開されました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-openssh-rce-2024

## 改訂履歴

| バージョン | 説明 | セクション | ステータス | 日付 |
|---|---|---|---|---|
| 1.8 | 現在調査中の製品、該当すると判断された製品、脆弱性がないと判断された製品のリストを更新。 | 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 | 2024年7月12日 |
| 1.7 | 現在調査中の製品、該当すると判断され | 該当製品, 脆弱性が存在す | Interim | 2024年 |

| バージョン | 説明 | セクション | ステータス | 日付 |
|---|---|---|---|---|
| | た製品、脆弱性がないと判断された製品のリストを更新。 | る製品, 脆弱性を含んでいないことが確認された製品 | | 7月11日 |
| 1.6 | 現在調査中の製品、該当すると判断された製品、脆弱性がないと判断された製品のリストを更新。 | 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 | 2024年7月10日 |
| 1.5 | 現在調査中の製品、該当すると判断された製品、脆弱性がないと判断された製品のリストを更新。 | 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 | 2024年7月9日 |
| 1.4 | 現在調査中の製品、該当すると判断された製品、脆弱性がないと判断された製品のリストを更新。 | 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 | 2024年7月8日 |
| 1.3 | 現在調査中の製品、該当すると判断された製品、脆弱性がないと判断された製品のリストを更新。 | 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 | 2024年7月5日 |
| 1.2 | 現在調査中の製品、該当すると判断された製品、脆弱性がないと判断された製品のリストを更新。 | 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 | 2024年7月4日 |
| 1.1 | 現在調査中の製品、該当すると判断された製品、脆弱性がないと判断された製品のリストを追加。Snortルールを追加。 | 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、詳細 | Interim | 2024年7月3日 |
| 1.0 | 初回公開リリース | — | Interim | 2024年7月2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。