OpenSSH サーバーにおける認証なしでのリモート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 : 2024-09-05 15:03
バージョン 1.14 : 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 社の脅威調査部門（TRU）が、glibc ベースの Linux システムの OpenSSH サーバー（sshd）に影響を与える、認証なしでの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。クライアントが LoginGraceTime 秒（デフォルトでは 120、古いバージョンの OpenSSH では 600）以内に認証されない場合、sshd SIGALRM ハンドラが非同期に呼び出されます。ただし、このシグナルハンドラは、非同期信号に対して安全ではないさまざまな関数（syslog() など）を呼び出します。

この脆弱性の説明については、『Qualys Security Advisory』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、製品ラインを調査しました。

このアドバイザリは、影響を受けるソフトウェアコンポーネントを含むことが判明しており、脆弱性が存在する可能性があるシスコ製品およびサービスのみを記載しています。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。本件は継続中の調査であるため、現在は脆弱性がないと判断された製品でも、追加情報が公開されることで今後脆弱性があると判断される可能性があります。

「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。

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。このアドバイザリが最終（Final）とマークされたら、関連する Cisco Bug を参照して詳細を確認してください。

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	9.18.4.34 9.20.3
Firepower 4100/9300 FXOS Firepower Chassis Manager	CSCwk62297	2.12.1
Firepower Management Center（FMC）ソフトウェア	CSCwk62296	7.0.6.3（2024 年 10 月） 7.2.8.1（2024 年 9 月） 7.4.2
Firepower Threat Defense（FTD）ソフトウェア	CSCwk62296	7.0.6.3（2024 年 10 月） 7.2.8.1（2024 年 9 月） 7.4.2
Identity Services Engine（ISE）	CSCwk61938	3.3 パッチ 3.2 パッチ 3.1 パッチ
Secure Access リソースコネクタ	CSCwk67866	2.0.0-2407032046
Cisco Secure Email and Web Manager	CSCwk63532	15.5.2 MR

Secure Email Gateway	CSCwk63523	15.5.2 MR 15.0.3 MR（2024 年 11 月） 16.0 (Oct 2024)
Cisco Secure Network Analytics	CSCwk64073	7.4.2 7.5.0
ネットワーク管理とプロビジョニング		
Application Policy Infrastructure Controller（APIC）	CSCwk62256	6.0(7x)（2024 年 9 月） 6.1(1x)（2024年9月）
Common Services Platform Collector（CSPC）	CSCwk62250	2.11.0.1
Crosswork Data Gateway	CSCwk62311	7.0.0
Cyber Vision	CSCwk62289	4.1.7 4.4.3 5.0.0
Cisco DNA Spaces コネクタ	CSCwk62273	コネクタ3
Evolved Programmable Network Manager（EPNM）	CSCwk62268	
Nexus Dashboard,（旧称：Application Services Engine）	CSCwk62261	3.2.1
Prime インフラストラクチャ	CSCwk62276	3.10.5
Smart PHY	CSCwk62284	24.2（2024 年 9 月）
Smart Software Manager オンプレミス	CSCwk62288	9-202407
仮想インフラストラクチャ マネージャ	CSCwk62277	5.0.1
Routing and Switching - Enterprise and Service Provider		
8000 シリーズ ルータ	CSCwk62108	24.3.1（2024 年 9 月） 24.2.2（2024 年 10 月） 24.2.11（SMU ID AA35431 から利用可能）
ASR 5000 シリーズ ルータ	CSCwk63293	
Catalyst IE3x00 高耐久性シリーズ スイッチ	CSCwk67488	17.15
Catalyst IE9300 高耐久性シリーズ スイッチ	CSCwk67488	17.15
エンベデッドサービス 3300 シリーズ スイッチ	CSCwk67488	17.15
GGSN Gateway GPRS Support Node	CSCwk63293	
NETCONF が有効になっている IOS XE ソフトウェア	CSCwk61216	17.15.1
IOS XRd コントロールプレーン	CSCwk62108	24.3.1（2024 年 9 月）

		24.2.2（2024 年 10 月） 24.2.11（SMU ID AA35431 から利用可能）
IOS XRd vRouters	CSCwk62108	24.3.1（2024 年 9 月） 24.2.2（2024 年 10 月） 24.2.11（SMU ID AA35431 から利用可能）
IP Services Gateway（IPSG）	CSCwk63293	
MDS 9000 シリーズ マルチレイヤ スイッチ	CSCwk62258	9.4(2a)
MME モビリティ マネジメント エンティティ	CSCwk63293	
NCS540L イメージを実行している Network Convergence System 540 シリーズ ルータ	CSCwk62108	24.3.1（2024 年 9 月） 24.2.2（2024 年 10 月） 24.2.11（SMU ID AA35431 から利用可能）
Network Convergence System 1010	CSCwk62108	24.3.1（2024 年 9 月） 24.2.2（2024 年 10 月） 24.2.11（SMU ID AA35431 から利用可能）
Network Convergence System 1014	CSCwk62108	24.3.1（2024 年 9 月） 24.2.2（2024 年 10 月） 24.2.11（SMU ID AA35431 から利用可能）
Network Convergence System 2000 シリーズ	CSCwm05826	10.82
Network Convergence System 5700 固定シャーシ NCS-57B1、NCS-57C1、および NCS-57D2	CSCwk62108	24.3.1（2024 年 9 月） 24.2.2（2024 年 10 月） 24.2.11（SMU ID AA35431 から利用可能）
Nexus 3000 シリーズ スイッチ	CSCwk61235	10.2(9)（2025 年 1 月） 10.3(6) 10.4(4)（2024 年 10 月） 10.5(1)
ACI モードの Nexus 9000 シリーズ ファブリック スイッチ	CSCwk62257	16.1(1) 16.0(7x)（2024 年 9 月）
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(9)（2025 年 1 月） 10.3(6) 10.4(4)（2024 年 10 月） 10.5(1)
ONS 15454 シリーズ マルチサービス プロビジョニング プラットフォーム	CSCwm05826	10.82

PDSN/HA Packet Data Serving Node and Home Agent	CSCwk63293	
PGW Packet Data Network Gateway	CSCwk63293	
System Architecture Evolution Gateway（SAEGW）	CSCwk63293	
Ultra Cloud Core：アクセスおよびモビリティ管理機能	CSCwk62243	
Ultra Cloud Core：セッション管理機能	CSCwk62246	2024.03.1.12
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	2024.03.1.12
Ultra Cloud Core 5G ポリシー制御機能	CSCwk62244	
Ultra Packet Core	CSCwk63293	
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 ストレージサーバー - Integrated Management Controller（CIMC）	CSCwk62266	4.3.4.241063 4.3.2.240077
UCS Director	CSCwk62255	6.9.1.0（2024 年 10 月）
UCS マネージャ	CSCwk62264	4.2(3l)（2024 年 9 月） 4.3(5a)（2024 年 10 月） 4.3(4c)
音声およびユニファイド コミュニケーション デバイス		
Desk Phone 9841	CSCwk62323	3.2(1)（2024 年 10 月）
Desk Phone 9851	CSCwk62323	3.2(1)（2024 年 10 月）
Emergency Responder	CSCwk63694	15.0.1.12900（2024 年 9 月） 15SU2（2024 年 9 月） ciscocm.V14_CVE-2024-6387_v1.1.zip[1] ciscocm.V15_CVE-2024-6387_v1.1.zip[1]
Prime Collaboration Deployment	CSCwk64755	15.0.1.12900（2024 年 9 月） 15SU2（2024 年 9 月） ciscocm.V14_CVE-2024-6387_v1.1.zip[1]

		ciscocm.V15_CVE-2024-6387_v1.1.zip[1]
Unified Communications Manager/Unified Communications Manager Session Management Edition	CSCwk62318	15.0.1.12900（2024 年 9 月） 15SU2（2024 年 9 月） ciscocm.V14_CVE-2024-6387_v1.1.zip[1] ciscocm.V15_CVE-2024-6387_v1.1.zip[1]
Unified Communications Manager IM and Presence Service	CSCwk63634	15.0.1.12900（2024 年 9 月） 15SU2（2024 年 9 月） ciscocm.V14_CVE-2024-6387_v1.1.zip[1] ciscocm.V15_CVE-2024-6387_v1.1.zip[1]
Unity Connection	CSCwk63494	15.0.1.12900（2024 年 9 月） 15SU2（2024 年 9 月） ciscocm.V14_CVE-2024-6387_v1.1.zip[1] ciscocm.V15_CVE-2024-6387_v1.1.zip[1]
Video Phone 8875	CSCwk62317	2.3(1) (Nov 2024)
Webex ビデオ メッシュ	CSCwk80951	
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	クラウド：RoomOS 11.18.1.6 オンプレミス：RoomOS 11.17.3.0 オンプレミス：RoomOS 11.14.4
Cisco Meeting Server	CSCwk62286	SMU - CMS 3.9.2（2024年9月） SMU - CMS 3.8.2（2024年9月）

Desk シリーズ	CSCwk70371	クラウド：RoomOS 11.18.1.6 オンプレミス：RoomOS 11.17.3.0 オンプレミス：RoomOS 11.14.4
Expressway シリーズ	CSCwk61630	X15.0.3 X15.2.0（2024 年 9 月）
Room シリーズ	CSCwk70371	クラウド：RoomOS 11.18.1.6 オンプレミス：RoomOS 11.17.3.0 オンプレミス：RoomOS 11.14.4
TelePresence Video Communication Server（VCS）	CSCwk61630	X15.0.3 X15.2.0（2024 年 9 月）
Webex Board	CSCwk70371	クラウド：RoomOS 11.18.1.6 オンプレミス：RoomOS 11.17.3.0 オンプレミス：RoomOS 11.14.4
ワイヤレス		
6300 シリーズ エンベデッド サービス アクセス ポイント	CSCwk62269	17.15 17.9.6（2024年9月） 17.12.4
Aironet 802.11ac Wave 2 アクセスポイント	CSCwk62269	17.15 17.9.6（2024年9月） 17.12.4
Aironet 1540 シリーズ	CSCwk62269	17.15 17.9.6（2024年9月） 17.12.4
Aironet 1560 シリーズ	CSCwk62269	17.15 17.9.6（2024年9月） 17.12.4
Catalyst 9100 シリーズ アクセスポイント	CSCwk62269	17.15 17.9.6（2024年9月） 17.12.4
Catalyst 9800 シリーズ ワイヤレス コントロー	CSCwk61216	17.15.1

ラ		
Catalyst ESS9300 エンベデッド シリーズ スイッチ	CSCwk67488	17.15
Catalyst IW6300 Heavy Duty シリーズ アクセス ポイント	CSCwk62269	17.15 17.9.6（2024年9月） 17.12.4
Catalyst IW9165 Heavy Duty シリーズ	CSCwk62269	17.15 17.9.6（2024年9月） 17.12.4
Catalyst IW9165 高耐久性シリーズ	CSCwk62269	17.15 17.9.6（2024年9月） 17.12.4
Catalyst IW9167 Heavy Duty シリーズ	CSCwk62269	17.15 17.9.6（2024年9月） 17.12.4
コネクテッド モバイル エクスペリエンス	CSCwk62270	11.0.1-129
組み込みワイヤレスコントローラ	CSCwk61216	17.15.1
IEC6400 エッジ コンピューティング アプライアンス	CSCwk62290	1.0.2 1.1.0（2024 年 10 月）

1. COP ファイルは、Cisco TAC のサポートがなくてもダウンロードおよびインストールできます。これらの COP ファイルは、特定のリリースにのみ適用されます。
2. この製品のリリース10.8より前のリリースは、CVE-2006-5051の影響を受けます。CVE-2006-5051は、回帰によって再導入された元の脆弱性で、CVE-2024-6387(regreSSHion)として識別されています。リリース10.8以降に存在するOpenSSHバージョンは、CVE-2006-5051またはCVE-2024-6387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
- CX Cloud Agent

- Cisco Secure Workload

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 Center
- Catalyst Center アシュアランス
- Cisco Telemetry Broker
- Crosswork Change Automation
- Crosswork Health Insights
- Crosswork Zero Touch Provisioning（ZTP）
- Data Center Network Manager（DCNM）
- Modeling Labs
- Network Services Orchestrator（NSO）
- Policy Suite
- Prime Cable Provisioning
- Prime Network Registrar
- SecureX Orchestration Remote
- 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
- Carrier Routing System（CRS）
- Catalyst SD-WAN コントローラ（旧称 SD-WAN vSmart）
- Catalyst SD-WAN Manager（旧称、SD-WAN vManage）
- Catalyst SD-WAN Validator（旧称、SD-WAN vBond Orchestrator）
- 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している 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
- SD-WAN vEdge クラウドルータ
- SD-WAN vEdge ルータ

Unified Computing

- Intersight 管理モード（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
- 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）
- HyperFlex System
- Integrated Management Controller（IMC）Supervisor
- 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 - Cloud Connect
- Unified Contact Center Express（Unified CCX）
- Unified Customer Voice Portal（Unified CVP）
- Unified Intelligence Center
- Unified Intelligent Contact Management Enterprise
- Unified SIP Proxy ソフトウェア

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 DX80

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 Industrial Wireless 3700 シリーズ
- Aironet 1530 シリーズ
- Aironet 1550 シリーズ
- Aironet 1570 シリーズ
- Meraki 製品
- 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
- Armorblox
- 攻撃対象領域の管理
- Business Critical Services
- シスコ マネージド サービス プラットフォーム
- Cisco Secure Client
- Cisco University - 次世代ラーニング
- Cloud Native Application Observability
- Crosswork Cloud
- Customer Journey Platform R10
- データ サイエンス サービス
- DevNet クラウドサービス
- DevNet Sandbox
- eSIM Flex
- Intersight SaaS
- IoT Control Center
- IoT Operations Dashboard
- 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
- Observability Platform
- Panoptica
- Provider Connectivity Assurance（旧称 Skylight Performance Analytics）
- Secure Cloud Analytics
- Cisco Secure Email Cloud
- Secure Email Encryption Service（旧称 Registered Envelope Service）

- Cisco Secure Email Threat Defense
- Secure Endpoint
- Cisco Secure Malware Analytics
- Cisco Secure Workload SaaS
- Slido
- Smartlook
- Smart Software Manager
- UC 管理
- 超高信頼ワイヤレスバックホール
- ユーザー定義のネットワーク クラウド サービス
- Vidcast
- Webex Calling
- Webex Contact Center
- Webex Events
- Webex - Meetings - Messaging App - Calling
- WebEx Teams
- XDR

詳細

この脆弱性に対するシスコの対応

シスコは、CVE-2024-6387 の影響について、すべての製品とサービスを引き続き評価しています。この脆弱性のエクスプロイトを検出するため、シスコは次の Snort ルールをリリースしました。

- 33654
- 63659

SSH アクセスを信頼できるホストのみに制限することをお勧めします。インフラストラクチャ アクセス制御リスト（ACL）を適用して SSH サービスへのアクセスを防止する手順については、次のガイドを参照してください。

- 『Cisco Guide to Harden Cisco IOS Devices』の「Limit Access to the Network with Infrastructure ACLs」
- 『Cisco Guide to Securing NX-OS Software Devices』の「Limiting Access to the Network with Infrastructure ACLs」
- 『Cisco UCS Hardening Guide』の「Limit Network Access with ACLs on Routers and Firewalls」
- 『Cisco Firewall Best Practices』の「Securing the Management Plane」
- 『Cisco Firepower Threat Defense Hardening Guide』

追加の強化に関するドキュメントについては、「Tactical Resources」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 社の脅威調査部門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
1.14	ソフトウェアの修正に関する情報を更新	脆弱性が存在する製品	Interim	2024年9月5日

バージョン	説明	セクション	ステータス	日付
1.13	ソフトウェアの修正に関する情報を更新	脆弱性が存在する製品	Interim	2024 年 8 月 21 日
1.12	ソフトウェアの修正に関する情報、影響を受けると判断された製品のリスト、および脆弱性がないと判断された製品のリストを更新。	「脆弱性のある製品」および「脆弱性を含んでいないことが確認された製品」	Interim	2024 年 8 月 2 日
1.11	影響を受けると判断された製品のリスト、および脆弱性がないと判断された製品のリストを更新。	「脆弱性のある製品」および「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 26 日
1.10	現在調査中の製品、影響を受けると判断された製品、および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 19 日
1.9	現在調査中の製品、影響を受けると判断された製品、および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 16 日
1.8	現在調査中の製品、影響を受けると判断された製品、および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、影響を受けると判断された製品、および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 11 日
1.6	現在調査中の製品、影響を受けると判断された製品、および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、影響を受けると判断された製品、および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、影響を受けると判断	該当製品, 脆弱性が存在	Interim	2024 年 7

バージョン	説明	セクション	ステータス	日付
	された製品、および脆弱性がないと判断された製品のリストを更新。	する製品, 脆弱性を含んでいないことが確認された製品		月 8 日
1.3	現在調査中の製品、影響を受けると判断された製品、および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、影響を受けると判断された製品、および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、影響を受けると判断された製品、および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、脆弱性が存在し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。