

シスコ製品に影響するSpring Frameworkの脆弱性：2022年3月



アドバイザリーID : cisco-sa-java-spring-rce-Zx9GUc67 [CVE-2022-22965](#)

初公開日 : 2022-04-01 23:45

最終更新日 : 2023-02-09 15:14

バージョン 1.13 : Final

CVSSスコア : [9.8](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvv65984](#) [CSCwb70105](#)

[CSCwb43739](#) [CSCwb43328](#) [CSCwb43736](#)

[CSCwc96587](#) [CSCwb43738](#) [CSCwb43335](#)

[CSCwb43346](#) [CSCwb43327](#) [CSCwb43734](#)

[CSCwb84370](#) [CSCwb43331](#) [CSCwb43342](#)

[CSCwd75689](#) [CSCwb43332](#) [CSCwb44794](#)

[CSCwa79849](#) [CSCwb43345](#) [CSCwb69766](#)

[CSCwb43340](#)

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

2022年3月31日に、JDK 9以降で実行されるSpring MVCおよびSpring WebFluxアプリケーションに影響を与えるSpring Frameworkの、重大な脆弱性がリリースされました。

CVE-2022-22965:JDK 9+でのデータバインディングによるSpring Framework RCE

この脆弱性の説明については、[VMware Spring Framework セキュリティ脆弱性レポート](#)を参照してください。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-java-spring-rce-Zx9GUc67>

該当製品

シスコは製品ラインを調査して、この脆弱性により影響を受ける可能性がある製品を特定しました。

「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。

このアドバイザリの「影響を受ける製品」セクションに記載されていない製品は、脆弱性が存在しないと判断されています。

脆弱性のある製品

シスコは製品ラインを調査して、この脆弱性により影響を受ける可能性がある製品を特定しました。

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。

製品	Cisco Bug ID	Fixed Release Availability
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		
Cisco CX Cloud Agent ソフトウェア	CSCwb41735	2.0 (Available)
ネットワーク管理とプロビジョニング		
Cisco Automated Subsea Tuning	CSCwb43658	2.1.0 (2022 年 5 月 31 日)
Cisco Crosswork Network Controller	CSCwb43703	3.0.2 (入手可能) 2.0.2 (入手可能)
Cisco Crosswork 最適化エンジン	CSCwb43709	3.1.1 (入手可能) 2.1.1 (入手可能)
Cisco Crosswork Zero Touch Provisioning (ZTP)	CSCwb43706	3.0.2 (入手可能) 2.0.2 (入手可能)
Cisco DNA Center	CSCwb43650	2.3.3.3 (2022 年 6 月 17 日) 2.2.3.6 (2022 年 6 月 6 日) 2.2.2.9 (2022 年 6 月 6 日)
Cisco Evolved Programmable Network Manager	CSCwb43643	6.0.1.1 (入手可能) 5.1.4.1 (入手可能) 5.0.2.3 (入手可能)
シスコ マネージド サービス アクセラレータ (MSX)	CSCwb43667	4.2.3 (入手可能)

Cisco Optical Network Planner	CSCwb43691	4.2 (2022 年 5 月 31 日) 5.0 (2022 年 8 月 30 日)
Cisco WAN Automation Engine (WAE) Live	CSCwb43708	7.5.2.1 (入手可能) 7.4.0.2 (入手可能) 7.3.0.3 (入手可能)
Cisco WAN Automation Engine (WAE)	CSCwb43708	7.5.2.1 (入手可能) 7.4.0.2 (入手可能) 7.3.0.3 (入手可能)
Data Center Network Manager (DCNM)	CSCwb43637	11.5.4 (入手可能)
Nexus Dashboard Fabric Controller (NDFC)	CSCwb43637	12.1.1 (2022 年 6 月 30 日)
Routing and Switching - Enterprise and Service Provider		
シスコ オプティカル ネットワーク コントローラ	CSCwb43692	2.0 (2022 年 5 月 31 日)
Cisco ソフトウェアデファインド AVC (SD-AVC)	CSCwb43727	4.3.1 (2022 年 7 月 30 日) 4.4.0 (2022 年 11 月 30 日)
音声およびユニファイド コミュニケーション デバイス		
Cisco Enterprise Chat and Email	CSCwb45202	11.6 : 脆弱性なし。 12.0 (2022 年 6 月 6 日) 12.5 (2022 年 6 月 6 日) 12.6 ES2 (2022 年 6 月 6 日)
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		
Cisco Meeting Server	CSCwb43662	3.5.0 (入手可能) 3.4.2 (2022 年 5 月 31 日) 3.3.3 (2022 年 6 月 17 日)

脆弱性を含んでいないことが確認された製品

シスコは製品ラインを調査して、この脆弱性により影響を受ける可能性がある製品を特定しました。

このアドバイザリの「影響を受ける製品」セクションに記載されていない製品は、脆弱性が存在しないと判断されています。

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。

ケーブルデバイス

- シスコの継続的展開と自動化フレームワーク
- Cisco Prime Cable Provisioning

Collaboration and Social Media

- Cisco SocialMiner
- Cisco Webex アプリ (旧 Cisco Webex Teams)
- Cisco Webex ミーティング サーバ

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

- Cisco Wide Area Application Services (WAAS)

ネットワークおよびコンテンツ セキュリティ デバイス

- Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェア
- Cisco Firepower Device Manager (FDM)
- Cisco Firepower Management Center (FMC) ソフトウェア
- Cisco Firepower システム ソフトウェア
- Cisco Identity Services Engine (ISE)
- Cisco Secure Email Gateway (旧 E メール セキュリティ アプライアンス (ESA))
- Cisco Secure Email and Web Manager (旧 Cisco Content Security Management Appliance (SMA))
- Cisco Secure Network Analytics (旧 Cisco Stealthwatch)
- Cisco Security Manager
- Cisco Umbrella Active Directory (AD) コネクタ
- Cisco Umbrella ローミングクライアント
- Cisco 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

- Cisco Application Policy Infrastructure Controller (APIC)
- シスコビジネスプロセスの自動化
- Cisco CloudCenter Action Orchestrator
- Cisco CloudCenter コスト最適化ツール
- Cisco CloudCenter Suite Admin
- Cisco CloudCenter Workload Manager
- Cisco CloudCenter
- シスコ コラボレーションの監査および評価
- Cisco Common Services Platform Collector (CSPC)
- Cisco Connected Mobile Experiences
- Cisco Connected Pharma
- Cisco Crosswork Change Automation
- Cisco Crosswork データゲートウェイ

- Cisco Crosswork Network Automation
- Cisco Crosswork Situation Manager
- Cisco Elastic Services Controller (ESC)
- Cisco Extensible Network Controller (XNC)
- Cisco Intelligent Node (iNode) Manager
- Cisco IoT Field Network Director (旧称 : Connected Grid Network Management System)
- Cisco NCS 2000 シェルフ仮想化オーケストレータ (SVO)
- シスコ ネットワーク変更管理および構成管理
- Cisco Network Insights for Data Center
- Cisco Nexus Dashboard Data Broker (旧 Nexus Data Broker)
- Cisco Nexus Dashboard (旧 Cisco Application Services Engine)
- Cisco Nexus Insights
- Cisco Policy Suite for Mobile
- Cisco Policy Suite
- Cisco Prime Performance Manager
- Cisco Smart PHY
- Cisco ThousandEyes Endpoint エージェント
- Cisco ThousandEyes Enterprise エージェント
- Cisco Virtual Topology System - Virtual Topology Controller (VTC) VM

Routing and Switching - Enterprise and Service Provider

- Cisco ACI HTML5 vCenter プラグイン
- Cisco ASR 5000 シリーズ ルータ
- Cisco Enterprise NFV Infrastructure Software (NFVIS)
- Cisco GGSN Gateway GPRS Support Node
- Cisco IOx Fog Director
- Cisco IP Services Gateway (IPSG)
- Cisco MME モビリティ マネージメント エンティティ
- Cisco Mobility Unified Reporting and Analytics システム
- Cisco Network Convergence System 2000 シリーズ
- Cisco ONS 15454 Series Multiservice Provisioning Platforms
- Cisco PDSN/HA Packet Data Serving Node and Home Agent
- Cisco PGW Packet Data Network Gateway
- Cisco SD-WAN vManage
- Cisco System Architecture Evolution Gateway (SAEGW)
- Cisco Ultra Packet Core
- Cisco Ultra Services Platform

ルーティングおよびスイッチング - スモール ビジネス

- Cisco Businessダッシュボード

Unified Computing

- Cisco HyperFlex

音声およびユニファイド コミュニケーション デバイス

- Cisco BroadWorks
- Cisco Cloud Connect
- Cisco Emergency Responder
- Cisco Packaged Contact Center Enterprise
- Cisco Unified Attendant Console Advanced
- Cisco Unified Attendant Console Business Edition
- Cisco Unified Attendant Console Department Edition
- Cisco Unified Attendant Console Enterprise Edition
- Cisco Unified Attendant Console Premium Edition
- Cisco Unified Communications Manager IM & Presence Service
- Cisco Unified Communications Manager Session Management Edition
- Cisco Unified Communications Manager
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- Cisco Unified Customer Voice Portal
- Cisco Unified Intelligence Center
- Cisco Unity Connection
- Cisco Virtualized Voice Browser

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

- Cisco Expressway Series
- Cisco TelePresence Integrator C Series
- Cisco TelePresence MX Series
- Cisco TelePresence Management Suite プロビジョニング拡張機能
- Cisco TelePresence Management Suite
- Cisco TelePresence Precision カメラ
- Cisco TelePresence Profile Series
- Cisco TelePresence SX Series
- Cisco TelePresence System EX シリーズ
- Cisco TelePresence Video Communication Server (VCS)
- Cisco Touch
- Cisco Video Surveillance Operations Manager
- Cisco Vision Dynamic Signage Director
- Cisco Webex Board シリーズ

- Cisco Webex Desk シリーズ
- Cisco Webex Room Navigator
- Cisco Webex Room シリーズ

ワイヤレス

- Cisco Ultra Cloud Core : アクセスおよびモビリティ管理機能
- Cisco Ultra Cloud Core - ネットワーク リポジトリ機能
- Cisco Ultra Cloud Core : ポリシー制御機能
- Cisco Ultra Cloud Core : Redundancy Configuration Manager
- Cisco Ultra Cloud Core : セッション管理機能
- Cisco 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

- Cisco BroadCloud
- Cisco Industrial Asset Vision
- Cisco IoT Control Center
- Cisco IoT Operations Dashboard (IOTOC)
- Cisco Kinetic for Cities
- Cisco Registered Envelope Service
- Cisco Smart Collector - ライフサイクル管理
- Cisco Umbrella
- Cisco Unified Communications Manager Cloud
- Cisco Webex Cloud-Connected UC (CCUC)

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 Product Security Incident Response Team (PSIRT) は、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 익스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。

出典

この脆弱性は、2022 年 3 月 31 日に VMware によって公表されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-java-spring-rce-Zx9GUc67>

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.13	脆弱性が存在しない製品を更新。	該当製品	Final	2023年2月9日
1.12	修正済みリリースに関する情報を更新。	脆弱性が存在する製品	Final	2022 年 6 月 1 日
1.11	「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	Final	2022 年 4 月 29 日
1.10	「調査中の製品」、「脆弱性のある製品」、「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	Interim	2022 年 4 月 26 日
1.9	「調査中の製品」、「脆弱性のある製品」、「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	Interim	2022 年 4 月 21 日
1.8	「調査中の製品」、「脆弱性のある製品」、「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	Interim	2022 年 4 月 14 日
1.7	「調査中の製品」、「脆弱性のある製品」、「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	Interim	2022年 4 月 13 日
1.6	「調査中の製品」、「脆弱性のある製品」、「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	Interim	2022 年 4 月 12 日

バージョン	説明	セクション	ステータス	日付
1.5	「調査中の製品」、「脆弱性のある製品」、「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	Interim	2022 年 4 月 11 日
1.4	「調査中の製品」、「脆弱性のある製品」、「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	Interim	2022 年 4 月 7 日
1.3	「調査中の製品」、「脆弱性のある製品」、「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	Interim	2022 年 4 月 6 日
1.2	「調査中の製品」、「脆弱性のある製品」、「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	Interim	2022 年 4 月 5 日
1.1	「調査中の製品」、「脆弱性のある製品」、「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	Interim	2022 年 4 月 4 日
1.0	初回公開リリース	—	Interim	2022 年 4 月 1 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、単独の転載や意識を施した場合、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。