Apache Struts の脆弱性がシスコ製品に与える影響：2023 年 12月

アドバイザリーID : cisco-sa-struts-C2kCMkmT
初公開日 : 2023-12-12 16:00
最終更新日 : 2023-12-21 22:23
バージョン 1.6 : Final
CVSSスコア : 9.8
回避策 : No workarounds available
Cisco バグ ID : CSCwi45131

CVE-2023-50164

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

2023 年 12 月 7 日、Apache Struts の次の脆弱性が開示されました。

CVE-2023-50164：攻撃者は、ファイル アップロード パラメータを操作してパストラバーサルを有効にすることができ、状況によっては、リモートコード実行に使用できる悪意のあるファイルをアップロードする可能性があります。

この脆弱性については、Apache Software Foundation Security Bulletin の説明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-struts-C2kCMkmT

該当製品

シスコでは、この脆弱性の影響を受ける製品を特定するために、製品ラインを調査しました。

「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。

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、より詳細な情報については関連する Cisco バグを参照して下さい。

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		
Identity Services Engine（ISE）	0.CSCwi45131	リリース3.1以降は影響を受けません。 ホットフィックスISE 2.7パッチ10 ホットフィックスISE 3.0パッチ7 ホットフィックスISE 3.0パッチ8 サポート部門に問い合わせて、ホットフィックスを入手してください。

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記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

シスコは、この脆弱性が以下の製品には影響を与えないことを確認しました。

Collaboration and Social Media

- Customer Collaboration Platform（旧 SocialMiner）

ネットワークおよびコンテンツ セキュリティ デバイス

- Security Manager

ネットワーク管理とプロビジョニング

- Nexus Dashboard Fabric Controller（NDFC）は、以前は Data Center Network Manager（DCNM）と呼ばれていました。
- Prime Access Registrar
- Prime Collaboration Assurance
- Prime Collaboration Provisioning

- Prime インフラストラクチャ
- Prime License Manager
- Prime Service Catalog

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）
- Emergency Responder
- Enterprise Chat and Email
- Finesse
- Hosted Collaboration Mediation Fulfillment
- Packaged Contact Center Enterprise(PCCE)
- Unified Communications Manager IM および Presence Service（Unified CM IM&P）
- Unified Communications Manager（Unified CM）/ Unified Communications Manager Session Management Edition（Unified CM SME）
- Unified Contact Center Enterprise（Unified CCE）
- Unified Contact Center Enterprise - Live Data Server（Unified CCE - Live Data Server）
- 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
- Unity Connection
- Virtualized Voice Browser

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。

出典

これらの脆弱性は、2023 年 12 月 7 日に Apache ソフトウェア財団によって公表されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-struts-C2kCMkmT

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.6	修正済みソフトウェアの表を更新。	脆弱性が存在する製品	Final	2023-DEC-21
1.5	Cisco Unified SIP Proxy Softwareを脆弱な製品のリストから脆弱性が存在しない製品のリストに移動。「調査中の製品」セクションを削除し、脆弱性が存在しないことが確認された製品のリストを更新しました。	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	2023-DEC-19
1.4	調査中の製品、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のリストを更新。	「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	2023-DEC-18
1.3	調査中の製品、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のリストを更新。	「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	2023-DEC-15
1.2	調査中の製品、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のリストを更新。「脆弱性のある製品」セクションへの誤ったリンクを更新。	「調査中の製品」、「脆弱性が存在する製品」、「脆弱性が存	Interim	2023-DEC-14

バージョン	説明	セクション	ステータス	日付
		在しない製品」		
1.1	調査中の製品、脆弱性を含んでいないことが確認された製品のリストを更新。	調査中の製品と脆弱性が存在しないことが確認された製品	Interim	2023 年 12 月 13 日
1.0	初回公開リリース	—	Interim	2023 年 12 月 12 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。