Apache Struts のリモートでコードが実行される脆弱性がシスコ製品に与える影響： 2018 年 8 月

Critical

アドバイザリーID : cisco-sa-20180823-apache-struts

初公開日 : 2018-08-23 20:00

最終更新日 : 2018-09-17 18:52

バージョン 1.12 : Final

回避策 : No workarounds available

Cisco バグ ID :

CVE-2018-11776

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

Apache Struts の脆弱性により、認証されていないリモートの攻撃者がターゲット システム上で任意のコードを実行する可能性があります。

この脆弱性は、該当のソフトウェアによるユーザ入力の検証が不十分なことに起因します。これが原因で、名前空間値のない結果の使用や、値またはアクションのない *URL* タグの使用が可能になります。 上位アクションまたは設定にも名前空間がない、またはワイルドカードの名前空間がない場合、攻撃者は、悪意のある入力を伴う要求を該当のアプリケーションに送信し、そのアプリケーションに処理させることで、この脆弱性をエクスプロイトできる可能性があります。 不正利用が成功すると、攻撃者はターゲット システム上で該当アプリケーションのセキュリティ コンテキストで任意のコードを実行する可能性があります。

この脆弱性の不正利用の可能性を検出するため、次の Snort ルールを使用できます。 Snort SID 29639、39190、39191、および 47634

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180823-apache-struts

該当製品

「脆弱性のある製品」セクションで、該当す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。

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ない製品またはサービスは、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

アスタリスク（*）が付けられた脆弱性のある製品には、影響を受ける Struts ライブラリが含まれます。ただし、ライブラリの製品内での使用方法によっては、これらの製品は、発行時にシスコで認識されているエクスプロイト ベクトルのいずれに対しても脆弱性を示しません。

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。

Product	Cisco Bug ID	Fixed Release Availability
Collaboration and Social Media		
Cisco SocialMiner *	CSCvk78903	パッチは 2018 年 9 月 11 日から利用
Endpoint Clients and Client Software		
Cisco Prime サービス カタログ *	CSCvm13989	
Network and Content Security Devices		
Cisco Identity Services Engine（ISE）	CSCvm14030	パッチ ファイルは2018年8月31日か用可能
Voice and Unified Communications Devices		
Cisco Emergency Responder *	CSCvm14044	1151es（21-Sep-2018） スタンドアロン COPS（21-Sep-201
Cisco Finesse *	CSCvk78905	パッチ ファイルは 2018 年 9 月 7 日利用可能。
Cisco Hosted Collaboration Solution for Contact Center *	CSCvm14052	パッチ ファイル 利用可能 な 12-Sep 2018
Cisco MediaSense *	CSCvk78906	パッチ ファイル 利用可能 な 12-Sep 2018
Cisco Unified Communications Manager *	CSCvm14042	1151es および 1201es（14-Sep-201 スタンドアロン COPS（20-Sep-201
Cisco Unified Communications Manager IM & Presence Service（旧称 CUPS）*	CSCvm14049	1151es および 1201es（21-Sep-201 スタンドアロン COPS（20-Sep-201
Cisco Unified Contact Center Enterprise*	CSCvm13986	パッチ ファイル 利用可能 な 12-Sep 2018
Cisco Unified Contact Center Enterprise - Live Data server *	CSCvk78902	パッチ ファイルは 2018 年 9 月 7 日利用可能
Cisco Unified Contact Center Express *	CSCvm21744	パッチ ファイル 利用可能 な 12-Sep 2018
Cisco Unified Intelligence Center *	CSCvm13984	パッチ ファイル 利用可能 な 12-Sep 2018
Cisco Unified Intelligent Contact Management Enterprise*	CSCvm13986	パッチ ファイル 利用可能 な 12-Sep 2018
Cisco Unified SIP Proxy ソフトウェア *	CSCvm13980	918es（28-Sep-2018）
Cisco Unified Survivable Remote Site Telephony Manager *	CSCvm13979	パッチ ファイル 利用可能 な 12-Sep 2018
Cisco Unity Connection *	CSCvm14043	1151es および 1201su（18-Sep-201 スタンドアロン COPS（21-Sep-201
Cisco Virtualized Voice Browser *	CSCvm14056	パッチ ファイル 利用可能 な 12-Sep

		2018
Video, Streaming, TelePresence, and Transcoding Devices		
Cisco Video Distribution Suite for Internet Streaming (VDS-IS) *	CSCvm14027	2.3.35 (2018 年 9 月 15 日)
シスコ クラウド ホステッド サービス		
Cisco Network Performance Analysis	CSCvm14040	

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およびサービスのみが、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およびサービスには影響を与えないことを確認しました。次のリストにある製品ファミリのすべてのメンバーは、「脆弱性のある製品」セクションに明示的にリストされていない限り、この脆弱性の影響は受けないと判断されます。

ケーブル モデム

- Cisco 3G フェムトセル ワイヤレス

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 Data Center Network Manager

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 Secure Access Control System (ACS)

ネットワーク管理とプロビジョニング

- Cisco MXE 3500 Series Media Experience Engines
- Cisco Prime Access Registrar
- Cisco Prime Central for Service Provider
- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Provisioning
- Cisco Prime Infrastructure
- Cisco Prime LAN Management Solution - Solaris
- Cisco Prime License Manager
- Cisco Prime Network Registrar IP アドレス マネージャ (IPAM)
- Cisco Prime Network
- Cisco Prime Order Management
- Cisco Prime Provisioning
- Cisco Security Manager
- Cisco Smart Net Total Care - ローカル コレクタ アプライアンス

ルーティングおよびスイッチング - エンタープライズおよびサービス プロバイダー

- Cisco Broadband Access Center for Telco and Wireless

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
- Cisco Hosted Collaboration Mediation Fulfillment
- Cisco Unified Customer Voice Portal
- Cisco Unified E-Mail Interaction Manager
- Cisco Unified Web Interaction Manager
- Cisco Unity Express

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 Enterprise Content Delivery System (ECDS)
- Cisco Expressway Series
- Cisco TelePresence Video Communication Server（VCS）

シスコ クラウド ホステッド サービス

- Cisco Business Video Services Automation Software
- Cisco Cloud Web Security
- Cisco Deployment Automation Tool
- Cisco Network Device Security Assessment Service
- Cisco Services Provisioning Platform
- Cisco Smart Net Total Care - Contracts Information System Process Controller
- Cisco Smart Net Total Care
- Cisco Unified Service Delivery プラットフォーム
- Cisco Webex Meeting Center - Windows
- Cisco Webex Meeting Center
- Cisco Webex Network-Based Recording（NBR）Management
- Cisco Webex Teams（旧 Cisco Spark）
- クラウド & マネージド サービス プログラム（CMSP）

回避策

特定のシスコ製品またはサービスでの回避策は、製品固有またはサービス固有の 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。 Cisco Webex 環境に関する質問は、Cisco Technical Assistance Center（TAC）に送信できます。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts 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 TAC もしくは契約しているメンテナンス プロバイダーまで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、この脆弱性のエクスプロイト事例について認識しています。

出典

2018 年 8 月 22日現在、Apache Software Foundation は次のリンクにあるセキュリティ情報ページで、この脆弱性を一般に公開しています。 https://cwiki.apache.org/confluence/display/WW/S2-057

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180823-apache-struts

改訂履歴

Version	Description	Section	Status	日付
1.12	脆弱性が存在する製品のための情報 ソフトウェアアベイラビリティのアップデートしました。	該当製品	Final	2018-September-17
1.11	脆弱性が存在する製品のための情報 ソフトウェアアベイラビリティのアップデートしました。	該当製品	Final	2018-September-13
1.10	脆弱性が存在する製品のリストをアップデートしました; 前のバージョンでアスタリスクは不注意に省略されました。	該当製品	Final	2018 年 9 月 10 日
1.	脆弱性が存在する製品のための情報 ソフトウェアアベ	該当製品	Fi	2018

9	イラビリティのアップデートしました。		nal	年 9 月 6 日
1.8	脆弱性のある製品と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。 進行中の調査に対する参照を削除。	概要、該当製品	Final	2018 年 9 月 5 日
1.7	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。	該当製品	Interim	2018 年 9 月 4 日
1.6	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。	該当製品	Interim	2018 年 8 月 31 日
1.5	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。	該当製品	Interim	2018 年 8 月 30 日
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、エクスプロイト事例の認識を更新。	影響のある製品、エクスプロイト事例および公式発表	Interim	2018 年 8 月 29 日
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。	概要および該当製品	Interim	2018 年 8 月 28 日
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。	概要および該当製品	Interim	2018 年 8 月 28 日
1.1	Snort SID を追加。 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。	概要および該当製品	Interim	2018 年 8 月 24 日
1.0	初回公開リリース		Interim	2018 年 8 月 23 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。