Multiple Vulnerabilities in Apache Struts 2 Affecting Cisco Products: 2017 月 9 日

Critical

アドバイザリーID : cisco-sa-20170907-struts2

初公開日 : 2017-09-07 21:00

最終更新日 : 2017-10-23 20:27

バージョン 1.12 : Final

回避策 : No workarounds available

Cisco バグ ID :

CVE-2017-9793

CVE-2017-9804

CVE-2017-9805

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

2017 年 9 月 5 日、Apache ソフトウェア財団は、Apache Struts 2 パッケージの 3 つの脆弱性を公開するセキュリティ情報をリリースしました。 Apache ソフトウェア財団はこれらの脆弱性の 1 つを *Critical*、1 つを *Medium*、1 つを *Low* の重大度に分類しました 。 これらの脆弱性の詳細についてはこのアドバイザリの「 詳細情報」の項を参照してください。

シスコの複数の製品に、これらの脆弱性の影響を受けるバージョンの Apache Struts 2 パッケージが組み込まれています。

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 44315 および 44327 ~ 44330。

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-20170907-struts2

該当製品

製品がこの脆弱性による影響を受けるかどうかについては、このアドバイザリの「 脆弱性が存在する製品」および「 脆弱性を含んでいないことが確認された製品」の項を参照してください。 「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。 Bugs は Cisco Bug Search Tool で検索可能であり、利用可能な回避策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。

注:「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」の各項には Struts を含むシスコ製品のみがリストされています。 リストされていないシスコ製品には Struts は含まれておらず、したがっては影響を受けません。

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。 製品名の後にアスタリスク (*) が表示されている場合、製品は重大度が Critical である脆弱性 CVE-2017-9805 *Apache Struts REST plug-in XML processing arbitrary code execution vulnerability* に該当します。 公表時点で 4 つのシスコ製品が CVE-2017-9805 による影響を受けることが確認されています。

シスコは、この表に記載されている各シスコ バグに修正済みソフトウェア リリースに関する詳細情報を示しています。 Bugs は、 Cisco Bug Search Tool で検索できます。 ソフトウェア アップグレードを計画する際は、直接 Bugs を確認してください。最新情報が記載されています。

Product	Cisco Bug ID	Fixed Release Availability
Network Management and Provisioning		
Cisco Digital Media Manager	CSCvf86117	修正予定なし（EoSWM）（2016 年 19 日）
Cisco MXE 3500 Series Media Experience Engines (*)	CSCvf86119	修正予定なし（EoSWM）（2017 年 日）
Voice and Unified Communications Devices		
Cisco Hosted Collaboration Solution for Contact Center (*)	CSCvf86143	
Video, Streaming, TelePresence, and Transcoding Devices		
Cisco Video Distribution Suite for Internet Streaming（VDS-IS）(*)	CSCvf86124	Struts 2.3.34 を使用して製品を更新（2017 年 9 月 29 日）
Cisco Hosted Services		
Cisco Network Performance Analysis (*)	CSCvf86134	Struts 2.3.34 を使用して製品を更新（2017 年 9 月 12 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、以下の製品がこのアドバイザリに記載された脆弱性の影響を受けないことを確認しました。

Collaboration and Social Media

- Cisco Unified MeetingPlace
- Cisco WebEx Meetings Server

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 WebEx Management - SuperAdmin コントロール パネル

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 Identity Services Engine（ISE）
- Cisco Secure Access Control System（ACS）

ネットワーク管理とプロビジョニング

- Cisco Prime Access Registrar
- Cisco Prime Central for Service Provider
- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Provisioning
- Cisco Prime Home
- 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 Security Manager
- Cisco Smart Net Total Care - ローカル コレクタ アプライアンス
- Cisco Unified Intelligence Center

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 Business Edition 4000
- Cisco Emergency Responder
- Cisco Enterprise Chat and Email
- Cisco Finesse
- Cisco Hosted Collaboration Mediation Fulfillment
- Cisco MediaSense
- Cisco SocialMiner
- Cisco Unified Communications Manager IM & Presence Service（旧称 CUPS）
- Cisco Unified Communications Manager
- Cisco Unified Contact Center Enterprise - Live Data server

- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- Cisco Unified Customer Voice Portal
- Cisco Unified E-Mail Interaction Manager
- Cisco Unified Intelligent Contact Management Enterprise
- Cisco Unified SIP Proxy ソフトウェア
- Cisco Unified Survivable Remote Site Telephony Manager
- Cisco Unified Web Interaction Manager
- Cisco Unity Connection
- Cisco Unity Express
- 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 Enterprise Content Delivery System (ECDS)

シスコ ホステッド サービス

- Cisco Business Video Services Automation Software
- Cisco クラウド E メール セキュリティ
- Cisco Cloud Web Security
- Cisco Context Service
- Cisco Deployment Automation Tool
- Cisco Network Device Security Assessment Service
- Cisco Partner Support Service 1.x
- Cisco Prime サービス カタログ
- Cisco Services Provisioning Platform
- Cisco Smart Net Total Care - Contracts Information System Process Controller
- Cisco Smart Net Total Care
- Cisco Spark
- Cisco Tidal Performance Analyzer
- Cisco Umbrella
- Cisco Unified Service Delivery プラットフォーム
- Cisco WebEx Meeting Center - Windows
- Cisco WebEx Network-Based Recording (NBR) Management

詳細

Apache Struts REST Plug-In XML Processing Arbitrary Code Execution Vulnerability

Apache Struts の Representational State Transfer（REST）プラグインの脆弱性により、認証されていないリモート攻撃者が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、REST プラグインと該当ソフトウェアの XStream ハンドラによる XML 要求の逆シリアル化が不適切であることに起因します。 攻撃者は、巧妙に細工された XML コンテンツをターゲット システムに送信することにより、この脆弱性を不正利用する可能性があります。 不正利用が成功すると、攻撃者はシステム上で任意のコードを実行し、システムを完全に侵害する可能性があります。

この脆弱性には次の CVE ID が割り当てられています。 CVE-2017-9805

この脆弱性のセキュリティ影響評価（SIR）は *Critical* です。

Apache Struts REST Plug-In Denial of Service Vulnerability

Apache Struts の REST プラグインの脆弱性により、認証されていないリモートの攻撃者がターゲット システムにサービス妨害（DoS）状態を発生させる可能性があります。

この脆弱性は、該当アプリケーションの REST プラグインの *XStream* ライブラリによるユーザ指定入力の検証が不十分であることに起因します。 攻撃者は、該当システムに巧妙に細工した XML データを送信する可能性があります。 不正利用に成功すると、攻撃者はターゲット システムに DoS 状態を引き起こす可能性があります。

この脆弱性には次の CVE ID が割り当てられています。 CVE-2017-9793

この脆弱性の SIR は *Medium* です。

Apache Struts URLValidator Resource Exhaustion Denial of Service Vulnerability

Apache Struts の *URLValidator* 機能の脆弱性により、認証されていないリモートの攻撃者が該当システムにサービス妨害（DoS）状態を発生させる可能性があります。

この脆弱性は、該当ソフトウェアが *URLValidator* 機能を使用して URL を検証する際に、ユーザ指定入力の検証が不十分であることに起因します。 攻撃者は、Apache Struts の該当バージョンを利用するアプリケーションのフォーム フィールドで巧妙に細工された URL を送信することにより、この脆弱性を不正利用する可能性があります。 エクスプロイトは正規表現（regex）処理で *URLValidator* が過剰な量の CPU リソースを消費する条件を引き起こし、その結果 DoS 状態になる可能性があります。

この脆弱性には次の CVE ID が割り当てられています。 CVE-2017-9804

この脆弱性の SIR は *Low* です。

回避策

これらの脆弱性に対処する回避策は Cisco Bugs に記載され、 Cisco Bug Search Tool で検索できるようになります。

修正済みソフトウェア

該当ソフトウェア リリースへの更新プログラムは利用可能になった時点で公開され、それらの更新に関する情報は Cisco Bugs に記載されます。 Cisco Bug Search Tool を使用してアクセスできます。

シスコがこれらの脆弱性に対処するソフトウェア アップデートをリリースした際、そのアップデートをインストールしたり、関連するサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットのみとなります。 そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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 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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

脆弱性が存在する各製品の影響を受けるリリースと修正済みリリースを判別するには、このアドバイザリの 「 脆弱性が存在する製品」の項で製品を識別する Cisco Bug を参照してください。 Cisco Bugs は、 Cisco Bug Search Tool で検索できます。

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) では、シスコ製品に対するこの脆弱性の不正利用事例とその公表は確認しておりません。

CVE-2017-9805 *Apache Struts REST plug-in XML processing arbitrary code execution vulnerability* については、アクティブな不正利用が報告されています。 公開時点でこの不正利用は、潜在的に脆弱なシステムを識別しようとするスキャン アクティビティで主に観測されています。

出典

2017 年 9 月 5 日に Apache ソフトウェア財団は次のセキュリティ情報でこれらの脆弱性を公開しました。

- CVE-2017-9805： http://struts.apache.org/docs/s2-052.html
- CVE-2017-9804： http://struts.apache.org/docs/s2-050.html
- CVE-2017-9793： http://struts.apache.org/docs/s2-051.html

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170907-struts2

改訂履歴

Version	Description	Section	Status	日付
1.12	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し、Cisco Umbrella を追加。	脆弱性を含んでいないことが確認された製品	Final	2017 年 10 月 23 日
1.11	修正に関する情報を追加し、脆弱性が存在する製品の表を更新。 概要、影響を受ける製品、脆弱性が存在する製品、修正済みソフトウェアの文面を「最終版」に更新。	概要、影響を受ける製品、脆弱性が存在する製品、修正済みソフトウェア。	Final	2017 年 10 月 3 日
1.10	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。	脆弱性を含んでいないことが確認された製品	Interim	2017 年 9 月 28 日
1.9	脆弱性が存在する製品、脆弱性を含んでいない製品、調査中の製品の各項に含まれる製品リストを更新。	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interi	2017 年 9 月 25 日

			m	
1.8	脆弱性が存在する製品、脆弱性を含んでいない製品、調査中の製品の各項に含まれる製品リストを更新。	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017 年 9 月 21 日
1.7	脆弱性が存在する製品、脆弱性を含んでいない製品、調査中の製品の各項に含まれる製品リストを更新。 Under Affected Products added further clarification on products not listed.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017-September-18
1.6	脆弱性が存在する製品、脆弱性を含んでいない製品、調査中の製品の各項に含まれる製品リストを更新。	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017-September-15
1.5	脆弱性が存在する製品、脆弱性を含んでいない製品、調査中の製品の各項に含まれる製品リストを更新。	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017-September-14
1.4	脆弱性が存在する製品、脆弱性を含んでいない製品、調査中の製品の各項に含まれる製品リストを更新。	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017-September-13
1.3	脆弱性が存在する製品、脆弱性を含んでいない製品、調査中の製品の各項に含まれる製品リストを更新。	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017-September-12
1.2	脆弱性が存在する製品、脆弱性を含んでいない製品、調査中の製品の各項に含まれる製品リストを更新。	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017-September-11
1.1	脆弱性が存在する製品、脆弱性を含んでいない製品、調査中の製品の各項に含まれる製品リストを更新。 Added the SIR value for each vulnerability. Added information about public exploitation.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable, Details, Exploitation and Public Announcements	Interim	2017-September-08
1.0	初回公開リリース		Interim	2017-September-07

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。