Apache Struts2 ジャカルタ シスコ製品に影響を及ぼすマルチパート パーサー ファイル アップロード コード 実行脆弱性

Critical

アドバイザリーID : cisco-sa-20170310-struts2

初公開日 : 2017-03-10 19:30

最終更新日 : 2017-05-05 17:02

バージョン 1.12 : Final

回避策 : No workarounds available

Cisco バグ ID : CSCvd49788 CSCvd51442 CSCvd49817 CSCvd49829 CSCvd51443 CSCvd51283 CSCvd63318 CSCvd56593 CSCvd63325 CSCvd63328 CSCvd56191 CSCvd63322 CSCvd49841

CVE-2017-5638

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 3月 6 日で、Apache は攻撃者が巧妙に細工された *Content-Type*、*内容開封*、*または Content-Length 値の*使用によってターゲットのシステムでコマンドをリモートで実行することを可能にする可能性がある Apache Struts2 で使用されたジャカルタ マルチパート パーサーの脆弱性を表わしました。

この脆弱性は CVE-ID CVE-2017-5638 を割り当てられました。

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-20170310-struts2

該当製品

シスコでは、本脆弱性の影響を受ける製品と影響の範囲を特定するために、製品ラインを調査中です。 製品が影響を受けているかについて情報に関してはこのアドバイザリの 脆弱性が存在する製品および 脆弱性が存在しない製品セクションを参照して下さい。

「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。 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。

特定の修正済みソフトウェア バージョンに関する詳細情報はアドバイザリのこのセクションの脆弱性が存在する製品表にリストされている Ciscoバグで文書化されています。 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した場合、最新および最新情報があるのでバグを直接検討すること確実でであって下さい。

Product	Cisco Bug ID	Fixed Release Availability
Collaboration and Social Media		
Cisco SocialMiner	CSCvd63318	11.5 SU1（7-April-2017）
Network and Content Security Devices		
Cisco Identity Services Engine（ISE）	CSCvd49829	利用可能なパッチ（24-March-2017）
Network Management and Provisioning		
Cisco Prime License Manager	CSCvd51283	11.5(1)SU1a（今利用可能な）
Cisco Unified Intelligence Center	CSCvd56191	11.5(1) ES03（30-March-2017）
Voice and Unified Communications Devices		
Cisco Emergency Responder	CSCvd51442	11.5 のためのパッチ（19-April-2017）
Cisco Finesse	CSCvd63325	11.5 ES2（7-April-2017）
Cisco Hosted Collaboration Mediation Fulfillment	CSCvd51443	HCM-F 11.5.1 SU1（7-April-2017）
Cisco Hosted Collaboration Solution for Contact Center	CSCvd56593	10.5(3) 利用可能なパッチ 11.0(2)（22-March-2017） 11.5(1)（22-March-2017） 10.0(2)（24-March-2017）
Cisco MediaSense	CSCvd63328	11.5（7-April-2017）
Cisco Packaged Contact Center Enterprise	CSCvd51212	
Cisco Unified Communications Manager IM & Presence Service（旧称 CUPS）	CSCvd49842	利用可能なパッチ（23-March-2017）
Cisco Unified Communications Manager Session Management Edition	CSCvd49840	利用可能なパッチ（31-March-2017）
Cisco Unified Communications Manager	CSCvd49840	利用可能なパッチ（31-March-2017）
Cisco Unified Contact Center Enterprise - Live Data server	CSCvd63365	10.5(3)（利用可能） 11.0（2）（7-April-2017） 11.5(1)（7-April-2017） 10.0(2)（利用可能）
Cisco Unified Contact Center Enterprise	CSCvd51210	10.5(3)（利用可能） 11.0（2）（22-March-2017） 11.5(1)（22-March-2017 10.0(2)（24-March-2017）
Cisco Unified Contact Center Express	CSCvd63322	11.5 SU1（7-April-2017）
Cisco Unified Intelligent Contact Management Enterprise	CSCvd51210	10.5(3)（利用可能） 11.0（2）（22-March-2017）

		11.5(1)（22-March-2017 10.0(2)（24-Mar-2017）
Cisco Unified SIP Proxy ソフトウェア	CSCvd49788	10.1（6月 2017）
		12.0（27-Mar-2017）
Cisco Unity Connection	CSCvd49841	11.5（10-Apr-2017）
		11.0（10-Apr-2017）
Cisco Virtualized Voice Browser	CSCvd63333	11.5 SU1（7-April-2017）
Cisco Hosted Services		
Cisco Prime Service Catalog アプライアンスおよびバーチャル アプライアンス	CSCvd49817	PSC 12.0 パッチ 1（14-Mar-2017）

脆弱性を含んでいないことが確認された製品

Collaboration and Social Media

- Cisco Unified MeetingPlace
- Cisco WebEx Meetings クライアント-オン前提
- 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 Agent for OpenFlow
- Cisco AnyConnect Secure Mobility Client for Android
- Cisco AnyConnect Secure Mobility Client for Linux
- Mac OS X のための Cisco AnyConnect セキュア モビリティ クライアント
- Cisco AnyConnect Secure Mobility Client for Windows
- Cisco AnyConnect Secure Mobility Client for iOS
- Cisco Jabber クライアント フレームワーク（JCF）コンポーネント
- Cisco Jabber Guest
- Cisco Jabber Software Development Kit
- Cisco Jabber for Android
- Cisco Jabber for Mac
- Cisco Jabber for Windows
- Cisco NAC Agent for Windows
- Cisco NAC Agent
- Cisco WebEx Meetings for Android
- Windows 電話 8 のための Cisco WebEx Meetings

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 Network Device Security Assessment Service
- Cisco Visual Quality Experience Server
- Cisco Visual Quality Experience Tools Server
- 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 Adaptive Security Appliance（ASA）
- Cisco 内容セキュリティ アプライアンス モデル アップデート サーバ
- Cisco Content Security Management Appliance (SMA)
- Cisco Email Security Appliance (ESA)
- Cisco FX-OS ソフトウェア
- Cisco FireSIGHT システム ソフトウェア
- Cisco Secure Access Control System（ACS）
- Cisco Web Security Appliance (WSA)
- Lancope Stealthwatch Endpoint Concentrator
- Lancope Stealthwatch FlowCollector NetFlow
- Lancope Stealthwatch FlowCollector sFlow
- Lancope Stealthwatch FlowSensor
- Lancope Stealthwatch SMC
- Lancope Stealthwatch UDP Director

ネットワーク管理とプロビジョニング

- Cisco Application Networking Manager
- Cisco Application Policy Infrastructure Controller（APIC）
- Cisco Cloupia Unified Infrastructure Controller
- Cisco Configuration Professional
- Cisco DCNM
- Cisco Digital Media Manager
- Cisco MATE Collector
- Cisco MATE Design
- Cisco MATE Live
- Cisco 管理 アプライアンス
- Cisco Meeting Server
- Cisco Multicast Manager
- Cisco NetFlow Generation Appliance
- Cisco Network Analysis Module
- Cisco Packet Tracer
- Cisco Policy Suite
- Cisco Prime Access Registrar
- Cisco Prime Central エラー マネージャ
- Cisco Prime Central
- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Deployment
- Cisco Prime Collaboration Provisioning
- Cisco Prime Data Center Network Manager

- Cisco Prime Home
- Cisco Prime IP Express
- Cisco Prime Infrastructure
- Cisco Prime LAN Management Solution - Solaris
- Cisco Prime Network 変更および設定管理
- Cisco Prime Network Registrar IP アドレス マネージャ（IPAM）
- Cisco Prime Network Registrar
- Cisco Prime Network Services Controller
- Cisco Prime Network
- Cisco Prime Opticalサービス プロバイダー向け
- Cisco Prime Performance Manager
- Cisco Prime サービス カタログ
- Cisco Security Manager
- Cisco Smart Net Total Care - ローカル コレクタ アプライアンス
- Cisco Tidal Performance Analyzer
- Cisco UCS Central ソフトウェア
- スマートな接続されたホーム

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 ASR 5000 シリーズ
- Cisco Broadband Access Center for Telco and Wireless
- Cisco Connected Grid ルータ
- Cisco IOS XR ソフトウェア
- Cisco IOS および Cisco IOS XE ソフトウェア
- Cisco MDS 9000 Series Multilayer Switches
- Cisco Nexus 1000V InterCloud
- Cisco Nexus 1000V シリーズ スイッチ
- VMware vSphere 向け Cisco Nexus 1000V スイッチ
- Cisco Nexus 3000 Series Switches
- Cisco Nexus 4000 Series Blade Switches
- Cisco Nexus 5000 Series Switches
- Cisco Nexus 6000 Series Switches
- Cisco Nexus 7000 Series Switches
- Cisco Nexus 9000 シリーズ ファブリック スイッチ（ACI モード）
- Cisco Nexus 9000 シリーズ スイッチ（スタンドアロン、NX-OS モード）
- Cisco ONS 15454 Series Multiservice Provisioning Platforms
- Cisco Service Control Operating System
- Cisco Universal Small Cell 5000 シリーズ Cisco Universal Small Cell 7000 シリーズ
- Cisco ユニバーサル小さいセル Iuh

ルーティングおよびスイッチング - スモール ビジネス

- （Sx220）スイッチとスマートな Cisco 220 シリーズ
- Cisco 500 シリーズ スタック可能（Sx500）管理されたスイッチ
- Cisco スモール ビジネス 300 シリーズ（Sx300）はスイッチを管理しました

Unified Computing

- Cisco Common Services Platform Collector
- Cisco UCS 6200 シリーズ ファブリック インターコネクト
- Cisco UCS 6200 シリーズおよび 6300 シリーズ ファブリックは相互接続します
- Cisco UCS B シリーズ ブレード サーバ
- Cisco UCS Director
- Cisco UCS Manager
- Cisco UCS スタンドアロン Cシリーズ ラック サーバ- Integrated Management Controller
- Cisco Virtual Security Gateway for Microsoft Hyper-V
- Cisco Virtual Security Gateway

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 ATA 190 シリーズ アナログ ターミナル アダプタ
- Cisco Agent Desktop for Cisco Unified Contact Center Express
- Cisco Agent Desktop
- Cisco DX シリーズ IP フォン
- Cisco Enterprise Chat and Email
- Cisco IP Interoperability and Collaboration System (IPICS)
- Cisco Jabber for iPhone and iPad
- Cisco Paging Server（Informacast）
- Cisco Paging Server
- Cisco SPA112 2-Port Phone Adapter
- ルータとの Cisco SPA122 Analog Telephone Adapter（ATA）
- Cisco SPA232D マルチライン DECT Analog Telephone Adapter（ATA）
- Cisco SPA51x IP フォン
- Cisco SPA525G 5 行 IP 電話
- Cisco Small Business SPA300 シリーズ IP Phone
- Cisco Small Business SPA500 シリーズ IP Phone
- Cisco UC Integration for Microsoft Lync
- 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 Attendant Console Standard
- Cisco Unified Communications Domain Manager

- Cisco Unified Contact Center Domain Manager
- Cisco Unified Contact Center Management Portal
- Cisco Unified Customer Voice Portal
- Cisco Unified E-Mail Interaction Manager
- Cisco Unified IP 6945 電話
- Cisco Unified IP 7937 電話
- サードパーティ コール制御のための Cisco Unified IP 8831 会議電話
- Cisco Unified メッセージ ゲートウェイ
- Cisco Unified Survivable Remote Site Telephony Manager
- Cisco Unified Web Interaction Manager
- Cisco Unified Workforce Optimization -品質 管理 ソリューション
- Cisco Unified Workforce Optimization
- Cisco Unity Express
- Cisco Virtualization Experience Media Edition

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 4300 シリーズ Digital Media Player
- Cisco 4400 シリーズ Digital Media Player
- Cisco Cloud Object Storage
- Cisco DCM シリーズ D990x デジタル コンテンツ マネージャ
- Cisco Edge 300 Digital Media Player
- Cisco Edge 340 Digital Media Player
- Cisco Enterprise Content Delivery System (ECDS)
- Cisco Expressway Series
- Cisco MXE 3500
- Cisco TelePresence Conductor
- Cisco TelePresence Content Server
- Cisco TelePresence ISDN Gateway 3241
- Cisco TelePresence ISDN Gateway MSE 8321
- Cisco TelePresence ISDN Link
- Cisco TelePresence MCU 4200 シリーズ、4500 シリーズ、5300 シリーズ、MSE 8420、および MSE 8510
- Cisco TelePresence MX Series
- Cisco TelePresence Profile Series
- Cisco TelePresence SX Series
- Cisco TelePresence Serial Gateway Series
- Cisco TelePresence Server 7010 および MSE 8710
- 複数政党制メディア 310 および 320 の Cisco TelePresence Server
- 複数政党制メディア 820 の Cisco TelePresence Server
- Cisco TelePresence Server on Virtual Machine
- Cisco TelePresence Supervisor MSE 8050

- Cisco TelePresence System 1000
- Cisco TelePresence System 1100
- Cisco TelePresence System 1300
- Cisco TelePresence System 3000 Series
- Cisco TelePresence System 500-32
- Cisco TelePresence System 500-37
- Cisco TelePresence System EX シリーズ
- Cisco TelePresence システム TX1310
- Cisco TelePresence TX9000 シリーズ
- Cisco TelePresence Video Communication Server（VCS）
- Cisco Telepresence Integrator C
- Cisco VDS-IS
- Cisco Video Surveillance 3000 Series IP Cameras
- Cisco Video Surveillance 4000 Series High-Definition IP Cameras
- Cisco ビデオ サーベイランス 4300E および 4500E 高精細度 IP カメラ
- Cisco Video Surveillance 6000 Series IP Cameras
- Cisco Video Surveillance 7000 Series IP Cameras
- Cisco Video Surveillance Media Server
- Cisco Video Surveillance PTZ IP Cameras
- Cisco Videoscape AnyRes Live
- Cisco Videoscape Voyager Vantage
- Tandberg Codian ISDN ゲートウェイ 3210、3220、および 3240
- Tandberg Codian MSE 8320

ワイヤレス

- Cisco Aironet 1040 シリーズ アクセス ポイント
- Cisco Aironet 1130 AG シリーズ アクセス ポイント
- Cisco Aironet 1140 シリーズ アクセス ポイント
- Cisco Aironet 1200 シリーズ アクセス ポイント
- Cisco Aironet 1530 シリーズ アクセス ポイント
- Cisco Aironet 1550 シリーズ アクセス ポイント
- Cisco Aironet 1560 シリーズ アクセス ポイント
- Cisco Aironet 1570 シリーズ アクセス ポイント
- Cisco Aironet 1600 シリーズ アクセス ポイント
- Cisco Aironet 1700 シリーズ アクセス ポイント
- Cisco Aironet 1810 シリーズ OfficeExtend アクセス ポイント
- Cisco Aironet 1810w シリーズ アクセス ポイント
- Cisco Aironet 1815 シリーズ アクセス ポイント
- Cisco Aironet 1830 シリーズ アクセス ポイント
- Cisco Aironet 1850 シリーズ アクセス ポイント
- Cisco Aironet 2600 シリーズ アクセス ポイント

- Cisco Aironet 2700 シリーズ アクセス ポイント
- Cisco Aironet 2800 シリーズ アクセス ポイント
- Cisco Aironet 3500 シリーズ アクセス ポイント
- Cisco Aironet 3600 シリーズ アクセス ポイント
- Cisco Aironet 3700 シリーズ アクセス ポイント
- Cisco Aironet 3800 シリーズ アクセス ポイント
- Cisco Aironet 700 シリーズ アクセス ポイント
- Cisco Aironet 700W シリーズ アクセス ポイント
- Cisco Industrial Wireless 3700 シリーズ アクセス ポイント
- Cisco Mobility Services Engine
- Cisco ワイヤレス LAN コントローラ

シスコ ホステッド サービス

- Cisco Business Video Services Automation Software
- Cisco Cloud Web Security
- Cisco クラウドおよびシステム管理
- Cisco データセンター アナリティクス フレームワーク
- Cisco Deployment Automation Tool
- Ciscoネットワーク健全性フレームワーク
- Cisco Network Performance Analysis
- Cisco One Portal
- Cisco Partner Support Service 1.x
- Cisco Proactive Network Operations Center
- Cisco Registered Envelope Service
- Cisco Services Provisioning Platform
- Cisco Smart Care
- Cisco Smart Net Total Care - Contracts Information System Process Controller
- Cisco Smart Net Total Care -スマートな相互対話
- Cisco Smart Net Total Care
- Cisco Unified Service Delivery プラットフォーム
- Cisco ユニバーサル小さいセル CloudBase ファクトリ リカバリ ルート ファイルシステム
- Cisco WebEx Meeting Center
- Cisco WebEx Messenger Service
- Cisco WebEx ネットワーク ベース記録（NBR）管理
- OpenDNS
- SmartNet 合計注意

詳細

Apache Struts のジャカルタ マルチパート パーサーの脆弱性はリモート攻撃者非認証が影響を受

けたシステムの任意のコードを実行するようにする可能性があります。

脆弱性は影響を受けたソフトウェアのジャカルタ マルチパート パーサーに基づいてファイル アップロードを行うとき *コンテンツタイプ* ヘッダー値の不適当な処理が原因です。 攻撃者はターゲットとされたユーザの悪意のあるファイルをアップロードするように説得によってこの脆弱性を不正利用する可能性があります。 影響を受けたアプリケーションのジャカルタ マルチパート パーサーがファイルをアップロードすれば、攻撃者は任意のコードを実行する機能がある可能性があります。

セキュリティ侵害の痕跡

この脆弱性の不正利用の検出を助けるために Cisco は Cisco IPS シグニチャ SIG ID 7872-0 および Snort SID 41818、41819、41923、および 41922 をリリースしました。

回避策

利用可能な回避策は Cisco Bugs に記載されています。 Cisco Bug Search Tool で検索できます。

修正済みソフトウェア

シスコがリリースした無償ソフトウェア 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。
http://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。
http://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に対して、影響を受けるリリースと修正済みリリースを確認するには、製品によって特定される Cisco Bug を参照してください。 これらのバグは本アドバイザリの「脆弱性が存在する製品」の表に一覧されます。 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製品のセキュリティ上の問題に対する回答チーム（PSIRT）はシスコ製品に対するこのアドバイザリに説明がある脆弱性のあらゆる不正利用に気づいていません。

この脆弱性の公開エクスプロイトが入手可能です。

出典

この脆弱性は次のアドバイザリの Apache によって表われました:
https://cwiki.apache.org/confluence/display/WW/S2-045 および
https://cwiki.apache.org/confluence/display/WW/S2-046

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170310-struts2

改訂履歴

Version	Description	Section	Status	日付
1.12	Updated product lists.	脆弱性が存在する製品、脆弱性が存在しない製品	Final	2017-May-05
1.11	Updated product lists.	脆弱性が存在する製品、脆弱性が存在しない製品	Final	2017 年 4 月 19 日
1.10	Updated product lists.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Final	2017 年 4 月 13 日
1.9	Updated product lists.	Affected Products, Vulnerable Products,	Fin	2017-

		Products Confirmed Not Vulnerable	al	March-28
1.8	製品リストおよび要約およびソース情報アップデートしました。	要約、該当製品、脆弱性が存在する製品、脆弱性が存在しない製品、出典	Interim	2017-March-23
1.7	製品リストおよび Snort SID 情報をアップデートしました。	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable, Indicators of Compromise	Interim	2017-March-21
1.6	Updated product lists.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017 年 3 月 17 日
1.5	Updated product lists.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017 年 3 月 15 日
1.4	Updated product lists.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017-March-14
1.3	Updated product lists.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017-March-13
1.2	Updated product lists.	Affected Products, Products Confirmed Not Vulnerable	Interim	2017-March-13
1.1	Updated product lists.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017-March-11
1.0	初回公開リリース		Interim	2017-March-10

利用規約