Apache Struts 2 Command Execution Vulnerability in Multiple Cisco Products

Advisory ID: cisco-sa-20131023-struts2

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20131023-struts2

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。

Revision 1.1

Last Updated 2015 October 12 12:30 GMT

For Public Release 2013 October 23 16:00 UTC (GMT)

目次

要約

Apache Struts 2 コンポーネントが実装されている複数のシスコ製品が、リモート コマンド実行の脆弱性の影響を受けます。

この脆弱性は、ユーザによる入力の安全性を適切にチェックできないことに起因します。攻撃者は、OGNL（Object-Graph Navigation Language）式で構成された要求を巧妙に細工して該当システムに送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は標的のシステム上で任意のコードを実行できる可能性があります。

シスコは、この脆弱性に対処するため、Cisco Business Edition 3000 を除くすべての該当製品を対象とした無償のソフトウェア アップデートをリリースしました。Cisco Business Edition 3000 については、適用可能な対処法をシスコの担当者にお問い合わせください。

これらの脆弱性に対しては回避策がありません。このアドバイザリは、次のリンクで確認できま

す。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20131023-struts2

該当製品

脆弱性が認められる製品

次のシスコ製品のすべてのソフトウェア リリースが、この脆弱性の影響を受けます。

- Cisco Business Edition 3000
- Cisco Identity Services Engine (SE)
- Cisco Media Experience Engine (MXE) 3500 Series
- Cisco Unified SIP Proxy（Cisco Unified SP)
- Cisco Unified Contact Center Enterprise (Cisco Unified CCE) and Cisco Packaged Contact Center Enterprise (Cisco PCCE)

注： Cisco ISE ソフトウェアは、次のリンクの Cisco Security Advisory で説明されている別の脆弱性にも該当しています。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20131023-ise

Cisco ISE をご利用のお客様は、アップグレード パスを決定する前に、そちらのアドバイザリも参照してください。

脆弱性が認められない製品

分析の結果、次のシスコ製品は脆弱性の影響を受けないことがわかっています。

- 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 Business Edition 5000 および Cisco Business Edition 6000 シリーズ
- Cisco Cloud Web Security
- Cisco Conductor
- Cisco Configuration Assurance ソリューション
- Cisco Data Center Network Manager（DCNM）
- Cisco DVR
- Cisco Emergency Responder
- Cisco Firewall Service Module（FWSM）ソフトウェア
- Cisco Hosted Collaboration Mediation Fulfillment（HCM-F）
- Cisco Media Experience Engine（MXE）3000 シリーズおよび Cisco MXE 5600 シリーズ
- Cisco Prime Central for HCS Assurance
- Cisco Prime Infrastructure
- Cisco Prime LAN Management Solution（LMS）
- Cisco Prime Network Control System（NCS）
- Cisco Secure Access Control Server（ACS）
- Cisco TelePresence Manager、Cisco TelePresence Recording Server、Cisco TelePresence Multipoint Switch
- Cisco Unified Attendant Console
- Cisco Unified Communication Domain Manager（CUCDM）
- Cisco Unified Communication Manager（CallManager）
- Cisco Unified Communications Manager IM and Presence Service、Cisco Unified Presence

- Cisco Unified MeetingPlace
- Cisco Unified Operations Manager（CUOM）
- Cisco Unified Services Monitor（CUSM）
- Cisco Unified Survivable Remote Site Telephony（SRST）Manager
- Cisco Unified Survivable Remote Site Voicemail（SRSV）
- Cisco Unity Connection
- Cisco Videoscape Control Suite
- Cisco Web Security、Cisco Email Security、Cisco Content Security 管理アプライアンス
- Cisco WebEx
- Cisco WebEx Recording Format（WRF）、Cisco WebEx Network-Based Recorder（NBR）Player
- Cisco Wireless Control System (WCS)
- CiscoWorks Common Services

他のシスコ製品は、この脆弱性の影響を受けません。

詳細

DefaultActionMapper コンポーネントに存在する脆弱性により、認証されていないリモートの攻撃者が該当システムで任意のコマンドを実行できる可能性があります。

この脆弱性は、ユーザによる入力の安全性を適切にチェックできないことに起因します。攻撃者は、OGNL（Object-Graph Navigation Language）式で構成された要求を巧妙に細工してシステムに送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は標的のシステム上で任意のコードを実行できる可能性があります。

この脆弱性がシスコ製品に与える影響は、製品によって異なります。Cisco ISE、Cisco Unified SIP Proxy、Cisco Business Edition 3000 で脆弱性が不正利用されると、該当するシステムで任意のコマンドが実行される可能性があります。Cisco ISE および Cisco Unified SIP Proxy , Cisco Unified CCE, Cisco PCCE で攻撃を実行するのに認証は必要ありません。Cisco Business Edition 3000 でこの脆弱性を利用するには、攻撃者は自ら有効なクレデンシャルを用意するか、ユーザが有効なクレデンシャルを使って悪意のある URL を実行するように仕向ける必要があります。

Cisco MXE 3500 シリーズで不正利用に成功した攻撃者は、ユーザを別の Web サイト（おそらくは悪意のあるサイト）へリダイレクトすることはできますが、この製品では任意のコマンドを実行することはできません。

攻撃経路と影響の詳細については、このセキュリティ アドバイザリの「脆弱性スコア詳細」セクションを参照してください。

この脆弱性は、Cisco ISE については Cisco Bug ID CSCui22841（登録ユーザ専用）、Cisco Business Edition 3000 については CSCui33268（登録ユーザ専用）、Cisco Unified SIP Proxy については CSCui40582（登録ユーザ専用）、Cisco MXE 3500 シリーズについては CSCui48757（登録ユーザ専用）、Cisco Unified CCE and Cisco PCCE については CSCui51516 (登録 ユーザ専用) として文書化されています。

この脆弱性には Common Vulnerabilities and Exposures（CVE）ID として CVE-2013-2251 が割り当てられています。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコでは、基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x/

CSCui22841 - Cisco ISE Apache Struts 2 Remote Command Execution Vulnerability Calculate the environmental score of					
CVSS Base Score - **10.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - **8.3**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCui33268 - Cisco BE3000 Apache Struts 2 Remote Command Execution Vulnerability Calculate the environmental score of					
CVSS Base Score - **9.0**					
Acces	Access	Authentica	Confidenti	Integrit	Availabi

s Vector	Complexity	tion	ality Impact	y Impact	lity Impact
Network	Low	Single	Complete	Complete	Complete
CVSS Temporal Score - **7.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCui40582 - CUSP Apache Struts 2 Remote Command Execution Vulnerability Calculate the environmental score of					
CVSS Base Score - **10.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - **8.3**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCui48757 - Cisco MXE 3500 Apache Struts 2 Remote Command Execution Vulnerability Calculate the environmental score of					
CVSS Base Score - **4.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	None	Partial	None
CVSS Temporal Score - **3.3**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性がシスコ製品に与える影響は、製品によって異なります。Cisco ISE、Cisco Unified SIP Proxy、Cisco Business Edition 3000 で脆弱性が不正利用されると、該当するシステムで任意のコマンドが実行される可能性があります。Cisco ISE および Cisco Unified SIP Proxy で攻撃を実行するのに認証は必要ありません。Cisco Business Edition 3000 でこの脆弱性を利用するには、攻撃者は自ら有効なクレデンシャルを用意するか、ユーザが有効なクレデンシャルを使って悪意のある URL を実行するように仕向ける必要があります。

Cisco MXE 3500 シリーズで不正利用に成功した攻撃者は、ユーザを別の Web サイト（おそらくは悪意のあるサイト）へリダイレクトすることはできますが、この製品では任意のコマンドを実行することはできません。

ソフトウェア バージョンおよび修正

シスコは、この脆弱性に対処するため、Cisco Business Edition 3000 を除くすべての該当製品を対象とした無償のソフトウェア アップデートをリリースしました。Cisco Business Edition 3000 については、適用可能な対処法をシスコの担当者にお問い合わせください。

ソフトウェアのアップグレードを検討する場合は、http://www.cisco.com/go/psirt/ の Cisco Security Advisories, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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、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。

次の表に、該当する各製品に対する最初の修正リリースを記載します。

Product	First Fixed Release
Cisco ISE[1]	1.0.4.573-6, 1.1.0.665-4, 1.1.1.268-6, 1.1.2.145-9, 1.1.3.124-4, 1.1.4.218 and 1.2.0.899
Cisco Business Edition 3000	Not available - Please contact Cisco TAC or your Cisco representative fo available options
Cisco Unified SIP Proxy	8.5(5)
Cisco MXE 3500 Series	3.3.2 and apply StrutsPatch.zip
Cisco Unified CCE and Cisco PCCE	10.5(1), 8.5(4)ES37, 9.0(4)ES39, 9.0(3)ES13, 10.0(1)ES10, and 10.0(2)

注: Cisco Unified CCE のエンジニアリング スペシャル パッチ リリース は以下のリンクから入手可能です。

8.5(4):
http://www.cisco.com/cisco/software/special/release.html?config=2c8f679b8cdc4fed65e866e30fced34c
9.0(4):
http://software.cisco.com/download/special/release.html?config=b40f7ffb0a876e5dae4e202df4b6547b
9.0(3):
http://software.cisco.com/download/special/release.html?config=593487b10e77653c20560c54efa6e7a0

[1]Cisco ISE は、次のリンクの Cisco Security Advisory で説明されている別の脆弱性にも該当しています。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20131023-ise

Cisco ISE をご利用のお客様は、アップグレード パスを決定する前に、そちらのアドバイザリも参照してください。

回避策

この脆弱性を軽減する回避策はありません。

修正済みソフトウェアの入手

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

お客様がインストールしたりサポートを受けたりできるのは、ご購入いただいたフィーチャ セットに対してのみとなります。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、アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載の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。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、Cisco.com の Software Navigator からアップグレードを入手することができます。http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの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 Technical Assistance Center（TAC）に連絡してアップグレード ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- E メール：tac@cisco.com

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。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先（http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html）を参照してください。

不正利用事例と公式発表

Apache は、次の Web ページでこの脆弱性を確認しています：
http://struts.apache.org/release/2.3.x/docs/s2-016.html

この脆弱性を不正に利用するコードは、複数のソースからインターネットで一般に提供されています。プルーフオブコンセプト コードも、Apache Struts 2 の公式ページで公開されています。

Cisco Product Security Incident Response Team（PSIRT）では、該当するシスコ製品において、本アドバイザリに記載されている脆弱性のいかなる不正利用事例も確認しておりません。

Cisco Unified CCE および Cisco PCCE に対するこの脆弱性は Security Metrics の Kevin Ostrin 氏によってシスコに報告されました。.

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20131023-struts2

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の E メールで配信されています。

- cust-security-announce@cisco.com

- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.0	2015-October-09	Added information about Cisco Unified CCE and Cisco PCCE.
Revision 1.0	2013-October-23	Initial public release.

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関するサポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html を参照してください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。