Apache Struts 2 Command Execution Vulnerability in Multiple Cisco Products

Advisory ID: cisco-sa-20140709-struts2

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140709-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 1.2

Last Updated 2014 December 17 18:47 UTC (GMT)

For Public Release 2014 July 9 16:00 UTC (GMT)

目次

要約

複数のシスコ製品に実装されている Apache Struts 2 コンポーネントが、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 Apache によって特定されたものであり、Common Vulnerabilities and Exposures ID として CVE-2010-1870 が割り当てられています。

この脆弱性は、該当ソフトウェアの XWorks コンポーネントにおいて、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。このコンポーネントは、 *ParameterInterceptors* 指令を使用して、ホワイトリスト機能を介して実装される OGNL (Object-Graph Navigation Language) 式を解析します。攻撃者は、OGNL 式が含ま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 シリーズ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 シリーズをご利用のお客様は、適用可能な対処法についてシスコの担当者にお問い合わせください。

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。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-20140709-struts2

該当製品

脆弱性が認められる製品

次のシスコ製品はこの脆弱性の影響を受けます。

- Cisco Business Edition 3000 Series
- Cisco Identity Services Engine (ISE)
- Cisco Media Experience Engine (MXE) 3500 Series
- Cisco Unified Contact Center Enterprise (Cisco Unified CCE)

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 Adaptive Security Appliance (ASA) Software
- Cisco Business Edition 5000 Series and Cisco Business Edition 6000 Series
- Cisco Cloud Web Security (CWS)
- Cisco Conductor
- Cisco Configuration Assurance Solution (CAS)
- Cisco Prime Data Center Network Manager (DCNM)
- Cisco DVR
- Cisco Emergency Responder
- Cisco Firewall Service Module (FWSM) Software
- Cisco Hosted Collaboration Mediation Fulfillment (HCM-F)
- Cisco Media Experience Engine (MXE) 3000 Series and Cisco MXE 5600 Series
- Cisco Prime Central for Hosted Collaboration Solution (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, and Cisco TelePresence Multipoint Switch
- Cisco Unified Attendant Console
- Cisco Unified Communications Domain Manager (Cisco Unified CDM)
- Cisco Unified Communications Manager (Cisco Unified CM)
- Cisco Unified Communications Manager IM and Presence Service and Cisco Unified Presence
- Cisco Unified MeetingPlace
- Cisco Prime Unified Operation Manager (UOM)
- Cisco Prime Unified Services Monitor (USM)
- Cisco Unified SIP Proxy (USP)
- Cisco Unified Survivable Remote Site Telephony (SRST) Manager
- Cisco Unified Survivable Remote Site Voicemail (SRSV)

- Cisco Unity Connection
- Cisco Videoscape Control Suite Foundation (VCS-Foundation)
- Cisco Web Security Appliance (WSA), Cisco Email Security Appliance (ESA), and Cisco Content Security Management Appliance (SMA)
- Cisco WebEx
- Cisco WebEx Recording Format (WRF) and Cisco WebEx Network-Based Recorder (NBR) Player
- Cisco Wireless Control System (WCS)
- CiscoWorks Common Services (CS)

他のシスコ製品は、この脆弱性の影響を受けません。

詳細

Apache Struts 2 には脆弱性があり、認証されていないリモートの攻撃者がセキュリティの制限をバイパスして、該当システムにおいて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、該当ソフトウェアがユーザの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。認証されていないリモートの攻撃者は、巧妙に細工された OGNL（Object-Graph Navigation Language）式を送信してセキュリティの制限をバイパスし、サーバ側のオブジェクトで任意のコマンドを実行することで、この脆弱性を不正利用できる可能性があります。

この脆弱性を不正利用することで、Cisco Unified CCE に対して *Administrator* ユーザの権限でアクセスし、リモートからコードを実行できることが確認されています。Cisco ISE、Cisco MXE 3500、Cisco Business Edition 3000 シリーズで不正利用されることは理論的にはありえますが、再現することはできませんでした。この脆弱性の影響を受けるお客様は、修正済みのソフトウェア リリース バージョンにアップグレードすることを推奨します。

この脆弱性は、Cisco Business Edition 3000 シリーズについては Cisco bug ID CSCun31197（登録ユーザ専用）、Cisco ISE については CSCun31314（登録ユーザ専用）、Cisco MXE 3500 については CSCun31301（登録ユーザ専用）、Cisco Unified CCE については CSCun25241（登録ユーザ専用）として文書化されています。

Common Vulnerabilities and Exposures（CVE）ID として CVE-2010-1870 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

CSCun31197 - Cisco BE 3000 Apache Struts 2 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 - **7.6**					
Exploitability		Remediation Level		Report Confidence	
Unproven		Unavailable		Unconfirmed	

CSCun31314 - Cisco ISE Apache Struts 2 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 - **6.7**					
Exploitability		Remediation Level		Report Confidence	
Unproven		Official-Fix		Unconfirmed	

CSCun31301 - Cisco MXE 3500 Apache Struts 2 Command Execution Vulnerability Calculate the environmental score of					
CVSS Base Score - **10.0**					
Acces	Access	Authentica	Confidenti	Integrit	Availabi

s Vecto r	Comple xity	tion	ality Impact	y Impact	lity Impact
Netw ork	Low	None	Complete	Compl ete	Comple te
CVSS Temporal Score - **6.7**					
Exploitability		Remediation Level		Report Confidence	
Unproven		Official-Fix		Unconfirmed	

CSCun25241 - Cisco UCCE Apache Struts 2 Command Execution Vulnerability Calculate the environmental score of					
CVSS Base Score - **10.0**					
Acces s Vecto r	Access Comple xity	Authentica tion	Confidenti ality Impact	Integrit y Impact	Availabi lity Impact
Netw ork	Low	None	Complete	Compl ete	Comple te
CVSS Temporal Score - **8.3**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性が不正利用されると、該当するシステムでリモートからコードが実行される可能性があります。

この脆弱性を不正利用することで、Cisco Unified CCE に対して *Administrator* ユーザの権限でアクセスし、リモートからコードを実行できることが確認されています。Cisco ISE、Cisco MXE 3500、Cisco Business Edition 3000 シリーズで不正利用されることは理論的にはありえますが、再現することはできませんでした。この脆弱性の影響を受けるお客様は、修正済みのソフトウェア リリース バージョンにアップグレードすることを推奨します。

ソフトウェア バージョンおよび修正

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 Business Edition 3000 Series	Not available. Please contact Cisco TAC or your Cisco represer for available options.
Cisco Identity Services Engine (ISE)	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, 1.1.4.218-4, and 1.2.0.899
Cisco Media Experience Engine (MXE) 3500 Series	3.3.2 and apply StrutsPatch.zip
Cisco Unified CCE	10.5(1), 8.5(4)ES37, 9.0(4)ES39, 9.0(3)ES13

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、E 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/2.2.x/docs/s2-005.html

この脆弱性の不正利用を実演する機能コードが公開されています。

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不正利用事例とその公表は一切確認しておりません。

この脆弱性は、Cisco Unified CCE について Che-Chun Kuo 氏と Jason Sinchak 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-20140709-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
- fulldisclosure@seclists.org

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 1.2	2014-December-17	Credited vulnerability reporters, per request.
Revision 1.1	2014-August-27	Added additional information about fixed releases for Cisco Unified CCE.
Revision 1.0	2014-July-09	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/web/about/security/psirt/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。