Multiple Vulnerabilities in Cisco Unified MeetingPlace Solution

Advisory ID: cisco-sa-20130410-mp

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130410-mp/

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 1.0

For Public Release 2013 April 10 16:00 UTC (GMT)

目次

要約

Cisco Unified MeetingPlace アプリケーション サーバには認証バイパスに関する脆弱性が存在し、Cisco Unified MeetingPlace Web Conferencing サーバには任意のログインに関する脆弱性が存在します。いずれの脆弱性も不正利用に成功した場合、認証されていないリモートの攻撃者が 正当なユーザになりすまし、そのユーザの権限で該当システムに対して任意のコマンドを送信する可能性があります。

シスコはこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。Cisco Unified MeetingPlace Web Conferencing サーバにおける任意のログインに関する脆弱性に対しては回避策が存在します。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-20130410-mp/

該当製品

脆弱性が認められる製品

次の Cisco Unified MeetingPlace アプリケーション サーバ ソフトウェアのバージョンが、Cisco Unified MeetingPlace アプリケーション サーバにおける認証バイパスに関する脆弱性の影響を受けます。

Cisco Unified MeetingPlace Application Server Version	Affected
Prior to 7.0	No
7.0	Yes
7.1	Yes
8.0	Yes
8.5	Yes

Cisco Unified MeetingPlace アプリケーション サーバは、Cisco Unified MeetingPlace Web Conferencing サーバにおける任意のログインに関する脆弱性の影響を受けません。

次の Cisco Unified MeetingPlace Web Conferencing サーバ ソフトウェアのバージョンが Cisco Unified MeetingPlace Web Conferencing サーバにおける任意のログインに関する脆弱性の影響を受けます。

Cisco Unified MeetingPlace Web Conferencing Server Version	Affected
Prior to 7.0	No
7.0	Yes
7.1	Yes
8.0	Yes
8.5	Yes

Cisco Unified MeetingPlace Web Conferencing サーバは、[Remember Me] 認証オプションが有効になっている場合のみ、この脆弱性の影響を受けます。このオプションが有効になっているかを確認するには、[Home] > [Administration] > [Web Server] を表示します。[Web Server Customization Values] セクションの [Allow Remember Me] の値が [Yes] に設定されている場合、[Remember Me] オプションが有効になっており、システムはこの脆弱性の影響を受けます。

この [Remember Me] 認証オプションはデフォルトで有効になっています。

Cisco Unified MeetingPlace Web Conferencing サーバは、Cisco Unified MeetingPlace アプリケーション サーバにおける認証バイパスに関する脆弱性の影響を受けません。

注：バージョン 7.0 より前の Cisco Unified MeetingPlace アプリケーション サーバおよび Cisco Unified MeetingPlace Web Conferencing サーバのソフトウェアはソフトウェア メンテナンスが終了しています。7.0 より前のバージョンをご使用の場合は、サポートされているバージョンへのアップグレードに関してシスコ サポート チームにお問い合わせください。

Cisco Unified MeetingPlace Express について

Cisco Unified MeetingPlace Express は、Cisco Unified MeetingPlace アプリケーション サーバに

おける認証バイパスに関する脆弱性の影響を受けます。
Cisco Unified MeetingPlace Express はソフトウェア メンテナンス終了となっています。代替製品に関してシスコ サポート チームにお問い合わせください。

脆弱性が認められない製品

他のシスコ製品においてこの脆弱性の影響を受けるものは、現在確認されていません。

詳細

Cisco Unified MeetingPlace は、統合された音声、ビデオ、Web 会議をホストする機能を提供するオンプレミス会議ソリューションです。このソリューションは組織のプライベートな音声/データ ネットワーク およびエンタープライズ アプリケーションに直接統合されます。Cisco Unified MeetingPlace サーバは、 外部の人物が会議に参加できるようにインターネットからのアクセスが可能な状態で 導入することもできます。

Cisco Unified MeetingPlace アプリケーション サーバは Cisco Unified MeetingPlace ソリューションのコアであり、音声およびビデオ サービスのほか、ソリューションのその他コンポーネント全般をサポートします。 Cisco Unified MeetingPlace ソリューションのコンポーネントである Cisco Unified MeetingPlace Web Conferencing サーバによって、 ユーザが会議を管理し、アプリケーションやプレゼンテーションを共有することが可能になります。

Cisco Unified MeetingPlace アプリケーション サーバにおける認証バイパスに関する脆弱性

Cisco Unified MeetingPlace アプリケーション サーバ の Web サーバ コンポーネントの認証コードにおける脆弱性により、該当システムからユーザがログアウトした後に、認証されていないリモートの攻撃者がユーザ セッションを乗っ取る可能性があります。
この脆弱性は、ユーザがログアウトしたときに該当システムがユーザ セッションを無効にしないことに起因します。攻撃者は巧妙に細工された HTTP GET または POST リクエストを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。攻撃者が不正利用を成功させるには、すでにログアウトしたユーザの session cookie 値を知る必要があります。Cisco Unified MeetingPlace アプリケーション サーバは 30 分後に session cookie を自動的に無効にします。このため、攻撃者が攻撃できる時間が 30 分間あります。不正利用に成功した場合、攻撃者が正当なユーザになりすまし、そのユーザの権限で該当システムの機密性、整合性、可用性に障害を与える可能性があります。

この脆弱性は、Cisco Bug ID CSCuc64885 （ 登録ユーザ専用 ）として文書化され、Common Vulnerabilities and Exposures （CVE ）ID として CVE-2013-1168 が割り当てられています。

Cisco Unified MeetingPlace Web Conferencing サーバにおける任意のログインに関する脆弱性

Cisco Unified MeetingPlace Web Conferencing サーバの認証コードにおける脆弱性により、認証されていないリモートの攻撃者が正当なユーザになりすまし、該当するシステムに対し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、該当システムで [Remember Me] オプションが設定されている場合に、ユーザのクッキーに対する検証が不適切になることに起因します。攻撃者は巧妙に細工されたログイン リクエストを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。攻撃を実行するには、攻撃者が有効なユーザ名を知っている必要があります。 不正利用に成功した場合、攻撃者が正当なユーザになりすまし、そのユーザの権限で該当システムの機密性、整合性、可用性に障害を与える可能性があります。

注：この脆弱性は [Remember Me] オプションが設定されている Cisco Unified MeetingPlace Web Conferencing サーバのみに影響します。Microsoft Outlook Integration は認証サービスに Cisco

Unified MeetingPlace アプリケーション サーバを使用しており、この脆弱性の影響を受けません。

この脆弱性は、Cisco Bug ID CSCuc64846（ 登録ユーザ専用 ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2013-1169 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/

CSCuc64885 - Cisco Unified MeetingPlace Application Server Authentication Bypass Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.6**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	High	None	Complete	Complete	Complete
CVSS Temporal Score - **6.3**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCuc64846 - Cisco Unified MeetingPlace Web Conferencing Server Arbitrary Login Vulnerability Calculate the environmental score of

CVSS Base Score - **9.3**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	Complete	Complete	Complete
CVSS Temporal Score - **7.7**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

これらの脆弱性の不正利用に成功した場合、攻撃者が正当なユーザになりすまし、そのユーザの権限で該当システムに対して任意のコマンドを送信する可能性があります。

ソフトウェア バージョンおよび修正

シスコはこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。

Cisco Unified MeetingPlace アプリケーション サーバにおける認証バイパスに関する脆弱性

次の表に、Cisco Unified MeetingPlace アプリケーション サーバにおける認証バイパスに関する脆弱性を修正した Cisco Unified MeetingPlace アプリケーション サーバ ソフトウェア リリースに関する情報を示します。

Cisco Unified MeetingPlace Application Server Major Release	Cisco Unified MeetingPlace Application Server F Release
7.0	Migrate to 7.1MR1 Patch 2
7.1	7.1MR1 Patch 2
8.0	8.0MR1 Patch 1
8.5	8.5MR3 Patch 1

Cisco Unified MeetingPlace Web Conferencing サーバにおける任意のログインに関する脆弱性

次の表に、Cisco Unified MeetingPlace Web Conferencing サーバにおける任意のログインに関する脆弱性を修正した Cisco Unified MeetingPlace アプリケーション サーバ ソフトウェア リリースに関する情報を示します。

Cisco Unified MeetingPlace Web Conferencing Server Major Release	Cisco Unified MeetingPlace Web Conferencing S Fixed Release

7.0	Migrate to 7.1MR1 Patch 2
7.1	7.1MR1 Patch 2
8.0	8.0MR1 Patch 2
8.5	8.5MR3 Patch 1

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。

回避策

Cisco Unified MeetingPlace アプリケーション サーバの認証バイパスに関する脆弱性を緩和する回避策はありません。

[Remember Me] 認証オプションを無効にすることで Cisco Unified MeetingPlace Web Conferencing サーバにおける任意のログインに関する脆弱性を緩和することができます。[Remember Me] 認証オプションを無効にするには、[Home] > [Administration] > [Web Server] を表示して [Web Server Customization Values] セクションで [Allow Remember Me] の値を [No] に設定します。

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 ソフトウェアを入手できます。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。

多言語による各地の電話番号、説明、E メール アドレスなどの TAC の連絡先情報については、Cisco Worldwide Contact を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、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確認しておりません。

これらの脆弱性は、カスタマー サポート ケースの解決中に発見されたものです。

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-20130410-mp/

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	2013-April-10	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。シスコ セキュリティ アドバイザリについては、すべて http://www.cisco.com/go/psirt/ で確認できます。