Cisco TelePresence System Default Credentials Vulnerability

Advisory ID: cisco-sa-20130807-tp

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130807-tp

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 2013 August 7 16:51 UTC (GMT)

For Public Release 2013 August 7 16:00 UTC (GMT)

目次

要約

Cisco TelePresence System の脆弱性により、リモートの攻撃者が、デフォルトのクレデンシャルで作成されたユーザ アカウントを使用して Web サーバにアクセスする可能性があります。

この脆弱性は、インストール時に作成されるデフォルト ユーザ アカウントに起因します。攻撃者はこの脆弱性を悪用し、デフォルトのアカウント クレデンシャルを使用して Web サーバにリモート アクセスすることができます。デフォルトのクレデンシャルでログインした攻撃者に、システムのすべての管理者権限が付与される可能性もあります。

これらの脆弱性に対しては回避策があります。
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-20130807-tp

該当製品

脆弱性が認められる製品

1.10.1 以前のリリースの CiscoTelePresence System ソフトウェアを実行する Cisco TelePresence System シリーズ 500、13X0、1X00、3X00、30X0 がこの脆弱性の影響を受けます。また、6.0.3 以前のリリースの Cisco TelePresence System ソフトウェアを実行する Cisco TelePresence TX 9X00 シリーズもこの脆弱性の影響を受けます。

脆弱性が認められない製品

Cisco TelePresence Multipoint Switch（CTMS）、Cisco TelePresence Recording Server（CTRS）、および Cisco TelePresence Manager（CTSMan）は、この脆弱性の影響を受けません。
この脆弱性の影響を受ける他のシスコ製品は、現在確認されていません。

詳細

Cisco TelePresence ソリューションは、ネットワークを介して遠く離れた場所にいる同僚や顧客、パートナーとの臨場感のある対面式のコミュニケーションやコラボレーションを実現します。

Cisco TelePresence System ソフトウェアには、パスワード回復用の管理者アカウントがあり、デフォルトで有効になっています。この脆弱性の不正利用に成功した場合、リモートの攻撃者がデフォルトのクレデンシャルを使用してシステム構成や設定を変更し、対象のシステムを完全に制御することが可能になります。攻撃者はこのアカウントを使用して、HTTPS セッションによりシステム構成や設定を変更する可能性があります。

この脆弱性は、 Cisco Bug ID CSCui43128（ 登録ユーザのみ）として文書化され、CVE ID として CVE-2013-3454 が割り当てられています。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、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

CSCui43128 - Cisco TelePresence System Default Credentials 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 - **9.5**					
Exploitability		Remediation Level		Report Confidence	
High		Workaround		Confirmed	

影響

この脆弱性の不正利用に成功した場合、リモートの攻撃者がパスワード回復用のデフォルトのクレデンシャルを使用してシステム構成や設定を変更し、対象のシステムを完全に制御することが可能になります。

ソフトウェア バージョンおよび修正

シスコは、準備ができ次第、修正済みソフトウェアを提供する予定です。

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

この脆弱性を軽減する回避策があります。

Cisco Unified Communications Manager（Unified CM）に登録された Cisco TelePresence コーデックをご使用の場合は、次の回避策を利用できます。

1.[Cisco Unified CM Administration] にアクセスして [Device] > [Phone] を選択し、構成済みの Cisco TelePresence ユニットを検索して選択します。
2.[Secure Shell Information (ssh)] の下にある [ssh **helpdesk** User] を、デフォルトの「**helpdesk**」から「**pwrecovery**」に変更し、別のパスワードを選択します。

これにより、Cisco TelePresence ユニットに保存されている **pwrecovery** アカウントが上書きされ、デフォルトのパスワードを Cisco Unfied CM 管理者が作成したパスワードに変更できるようになります。

注：この変更を行っても **ssh** を介したパスワード回復は設計通りに機能しますが、回復機能を実行するには Cisco TelePresence ユニットへの物理アクセスが必要になります。 **ssh** アクセスでは、 **pwrecovery** アカウント用に更新されたパスワード情報を使用する必要があります。

3.Cisco TelePresence コーデックを再起動して、更新後の Cisco Unified CM 構成をダウンロードします。

再起動するたびにコーデックによって構成がダウンロードされるため、この回避策の有効性も持続します。

以上により、管理者クレデンシャルまたは Cisco Unified CM で新たに設定された **pwrecovery** クレデンシャルを知らないユーザは、GUI にアクセスできなくなります。デフォルトの **pwrecovery** クレデンシャルは機能を停止します。

Cisco Unified CM に登録されていない Cisco TelePresence コーデックを使用している場合は、対象システムに手動による介入を行って問題を回避する必要があります。この回避策の実行方法については、Cisco Technical Assistance Center（TAC）にお問い合わせください。

修正済みソフトウェアの入手

シスコは、準備ができ次第、修正済みソフトウェアを提供する予定です。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

不正利用の可能性について、お客様からシスコに直接報告がありました。PSIRT は、この脆弱性の広範な不正利用事例、および公式発表は存在していないと認識しています。

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-20130807-tp

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 1.1	2013-August-07	Change to CVSSv2 scoring
Revision 1.0	2013-August-07	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。