Cisco Security Advisory: Default Credentials for Root Account on Tandberg E, EX and C Series Endpoints

Advisory ID: cisco-sa-20110202-tandberg

http://www.cisco.com/warp/public/707/cisco-sa-20110202-tandberg.shtml

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 2011 February 2 1600 UTC (GMT)

目次

要約

TC4.0.0 より前のソフトウェア バージョンで稼働している Tandberg C シリーズ エンドポイントおよび E/EX パーソナル ビデオ ユニットは、デフォルトでパスワードなしの root 管理者アカウントが有効にされた状態で出荷されています。攻撃者がこのアカウントを使用して、アプリケーション構成やオペレーティング システム設定を変更する可能性があります。

このデフォルト パスワードの問題を解決するためにソフトウェアをアップグレードする必要はなく、該当するすべてのユーザは設定コマンドによって変更または無効にできます。このドキュメントで説明されている回避策は、root アカウントを無効にする方法またはパスワードを変更する方法を示しています。

このアドバイザリは次のリンクに掲載されます。 http://www.cisco.com/warp/public/707/cisco-sa-20110202-tandberg.shtml

該当製品

脆弱性が存在する製品

この脆弱性に該当するのは、C20、C40、C60、C90、E20、EX60、EX90 コーデックで稼働しているソフトウェアを含む、Tandberg C シリーズ エンドポイントおよび E/EX パーソナル ビデオ ユニットです。Tandberg ユニットのソフトウェア バージョンは、Web ベースのユーザ インターフェイス (UI) にログインするか、xStatus SystemUnit コマンドを使用することで確認できます。

Tandberg ソフトウェア バージョンの確認は、Web ブラウザでコーデックの IP アドレスを入力して認証を行い (デバイスが認証に対して設定されている場合) 、メニュー オプションから [System Info] を選択します。バージョン番号が [System Info] ボックスの [Software Version] ラベルのところに表示されます。

または、デバイスのアプリケーション プログラマ インターフェイスから xStatus SystemUnit コマンドを使用して、ソフトウェア バージョンを確認することもできます。そのコーデックで実行されているソフトウェア バージョンが [SystemUnit Software Version] ラベルのところに表示されます。xStatus SystemUnit の出力は、次のような結果を表示します。

```
xStatus SystemUnit
*s SystemUnit ProductType: "Cisco TelePresence Codec"
*s SystemUnit ProductId: "Cisco TelePresence Codec C90"
*s SystemUnit ProductPlatform: "C90"
*s SystemUnit Uptime: 597095
*s SystemUnit Software Application: "Endpoint"
*s SystemUnit Software Version: "TC4.0"
*s SystemUnit Software Name: "s52000"
*s SystemUnit Software ReleaseDate: "2010-11-01"
*s SystemUnit Software MaxVideoCalls: 3
*s SystemUnit Software MaxAudioCalls: 4
*s SystemUnit Software ReleaseKey: "true"
*s SystemUnit Software OptionKeys NaturalPresenter: "true"
*s SystemUnit Software OptionKeys MultiSite: "true"
*s SystemUnit Software OptionKeys PremiumResolution: "true"
*s SystemUnit Hardware Module SerialNumber: "B1AD25A00003"
*s SystemUnit Hardware Module Identifier: "0"
*s SystemUnit Hardware MainBoard SerialNumber: "PH0497201"
*s SystemUnit Hardware MainBoard Identifier: "101401-3 [04]"
*s SystemUnit Hardware VideoBoard SerialNumber: "PH0497874"
*s SystemUnit Hardware VideoBoard Identifier: "101560-1 [02]"
*s SystemUnit Hardware AudioBoard SerialNumber: "N/A"
*s SystemUnit Hardware AudioBoard Identifier: ""
*s SystemUnit Hardware BootSoftware: "U-Boot 2009.03-65"
*s SystemUnit State System: Initialized
*s SystemUnit State MaxNumberOfCalls: 3
*s SystemUnit State MaxNumberOfActiveCalls: 3
*s SystemUnit State NumberOfActiveCalls: 1
*s SystemUnit State NumberOfSuspendedCalls: 0
*s SystemUnit State NumberOfInProgressCalls: 0
```

```
*s SystemUnit State Subsystem Application: Initialized
*s SystemUnit ContactInfo: "helpdesk@company.com"
** end
```

脆弱性が存在しない製品

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

詳細

Tandberg デバイスは、イマーシブな環境、会議室、個人用デスクトップおよびホーム オフィスに Cisco TelePresence エンドポイントを提供する Cisco TelePresence System の一部です。C シリーズ エンドポイントは通常、Multipurpose Room System（多目的会議室用システム）として展開されるもので、E/EX パーソナル ビデオ ユニットはデスクトップ デバイスです。

これらデバイスは、通常の運用では必要のない高度なデバッグ向けに有効にされた root ユーザを含んでいます。root アカウントは、管理者アカウントおよびユーザ アカウントと同じではありません。TC 4.0.0 より前のソフトウェア バージョンでは、root ユーザがデフォルトで有効にされています。TC 4.0.0 より前のデフォルト設定では root ユーザに対してパスワードを設定していません。

デバイスが TC 4.0.0 にアップグレードされると、root ユーザは無効になります。Tandberg C シリーズ エンドポイントおよび E/EX パーソナル ビデオ ユニット向けのシステム ソフトウェアは、次の場所からダウンロードできます。 http://www.tandberg.com/support/video-conferencing-software-download.jsp?t=2 。その他のソフトウェア バージョンで root パスワードを設定または root ユーザを無効にする方法については、このアドバイザリの「回避策」のセクションを参照してください。

この脆弱性には CVE-2011-0354 という CVE ID 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。このセキュリティ 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手助けとなる標準ベースの評価法です。

シスコは基本評価スコア（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、個々のネットワークにおける脆弱性の影響度を導き出すことができます。

シスコは次の URL にて CVSS に関する FAQ を提供しています。

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

また、シスコは個々のネットワークにおける環境影響度を算出する CVSS 計算ツールを以下の URL にて提供しています。

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

Root account enabled by default with no password Calculate the environmental score of					
CVSS Base Score - **10**					
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	

影響

この脆弱性の不正利用に成功した場合、許可されていないユーザがアプリケーション構成やオペレーティング システム設定を変更したり、デバイスの完全な管理制御権を取得したり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

ソフトウェアのアップグレードを検討する際には、 http://www.cisco.com/go/psirt/ および本アドバイザリ以降に公開のアドバイザリも参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください。

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しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報が不明確な場合は、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

TC4.0.0 ソフトウェア バージョン以降は、デフォルト設定で root ユーザが無効にされています。root アカウントを無効にするには、管理者がアプリケーション プログラマ インターフェイスにログインし、systemtools rootsettings off コマンドを使用してアカウントを一時的に無効にするか、systemtools rootsettings never コマンドで root ユーザを常時無効にします。

root ユーザは高度なデバッグ向けに有効にされています。root ユーザが必要な場合、このアカウントが有効にされているときにはパスワードを設定しておく必要があります。これは、systemtools rootsettings on [password] コマンドによって行うことができます。

TC 4.0.0 以降のソフトウェア バージョンを実行しているデバイス

TC4.0.0 ソフトウェア バージョン以降は、デフォルト設定で root ユーザが無効にされています。root アカウントを無効にするには、管理者がアプリケーション プログラマ インターフェイスにログインし、systemtools rootsettings off コマンドを使用してアカウントを一時的に無効にするか、systemtools rootsettings never コマンドで root ユーザを常時無効にします。

root ユーザは高度なデバッグ向けに有効にされています。root ユーザが必要な場合、このアカウントが有効にされているときにはパスワードを設定しておく必要があります。これは、systemtools rootsettings on [password] コマンドによって行うことができます。

TC4.0.0 を実行しているデバイスのデフォルト設定では、管理者ユーザに対するパスワードが含まれていません。管理者アカウントに対するパスワードは、xCommand SystemUnit AdminPassword Set Password: [password] コマンドで設定します。

TC 4.0.0 より前のソフトウェア バージョンを実行しているデバイス

TC4.0.0 より前のソフトウェア バージョンを実行しているデバイスでは、root ユーザを無効にすることはできません。root アカウントに対するパスワードは、管理者アカウントと同じです。管理者パスワードは xCommand SystemUnit AdminPassword Set Password: [password] コマンドで設定します。

修正済みソフトウェアの入手

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。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に特有の問題に関してご確認下さい。

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、または Cisco.com ダウンロード サイトの http://www.cisco.com/public/sw-center/sw-usingswc.shtml に説明のあるその他の条項に従うことに同意したことになります。

ソフトウェアのアップグレードに関し、psirt@cisco.com もしくは security-alert@cisco.com にお問い合わせいただくことはご遠慮ください。

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、シスコのワールドワイド Web サイト上の Software Center 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

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、本脆弱性に関する適切な処置について指示と支援を受けてください。

回避策の効果は、使用製品、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のお客様の状況に依存します。影響製品が多種多様であるため、回避策を実際に展開する前に、対象とするネットワークで適用する回避策が最適であるか、お客様のサービス プロバイダーやサポート会社にご相談ください。

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 Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。TAC の連絡先は次のとおりです。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このお知らせの 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に対する無償アップグレードは、TAC 経由でご要求いただく必要があります。

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、 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

この脆弱性は、 2600 Magazine の第 3 号第 27 巻で発表された「Hacking and Securing the Tandberg C20」で討論されています。

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。またシスコシステムズ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

本アドバイザリは、次のシスコのワールドワイド Web サイト上に掲載されます。

http://www.cisco.com/warp/public/707/cisco-sa-20110202-tandberg.shtml

ワールドワイド Web 以外にも、次の電子メールおよび Usenet ニュースの受信者向けに、この通知のテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで投稿されています。

- 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
- comp.dcom.sys.cisco@newsgate.cisco.com

このアドバイザリに関する今後の更新は、いかなるものもシスコのワールドワイド Web サイトに掲載される予定です。 しかしながら、前述のメーリング リストもしくはニュースグループに対し 積極的に配信されるとは限りません。この問題に関心があるお客様は上記 URL にて最新情報をご確認いただくことをお勧めいたします。

更新履歴

Revision 1.0	2011-Feb-02	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支援、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について詳しく知るには、シスコ ワールドワイド Web サイトの http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。このページには、シスコのセキュリティ通知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。