Cisco TelePresence System Integrator CシリーズおよびCisco TelePresence EXシリーズデバイスのデフォルトのルートアカウント製造エラー

アドバイザリーID : cisco-sa-20111109-telepresence-c-ex-series
初公開日 : 2011-11-09 16:00
最終更新日 : 2011-11-15 15:45
バージョン 1.2 : Final
回避策 : No Workarounds available
Cisco バグ ID :

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。

概要

Cisco TelePresence System Integrator CシリーズおよびCisco TelePresence EXシリーズのデバイス上で稼働するソフトウェアは、TC4.0リリース以降、セキュアなデフォルト設定を含むように更新されています。この変更に伴い、Cisco Security Advisory cisco-sa-20110202-tandbergがリリースされました。

2010年11月18日から2011年9月19日の期間中に出荷されたCisco TelePresence System Integrator CシリーズおよびCisco TelePresence EXシリーズのデバイスで、製造上の誤りにより、rootアカウントが有効になっている場合があります。

該当するデバイスの識別方法については、このアドバイザリの「詳細」セクションを参照してください。

この問題の修復方法については、このアドバイザリの「回避策」セクションを参照してください。

このアドバイザリは、 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111109-telepresence-c-ex-series で公開されています。

該当製品

次の製品は、2010年11月18日から2011年9月19日の間にソフトウェアリリースTC4.0、TC4.1、またはTC4.2で配布された場合にのみ影響を受けます。

脆弱性のある製品

指定された期間内に出荷されたCisco TelePresence System Integrator Cシリーズ、Cisco TelePresence EXシリーズ、およびCisco TelePresence Quick Set製品はすべて影響を受ける可能性があります。管理者は、http://serialnumbervalidation.com/PSIRT-20111026にあるシリアル番号検証ツールを使用して、デバイスのステータスを確認できます。

Serial Number Validatorツールは、製品の出荷時にデバイスが該当していたかどうかを示します。工場出荷時状態へのリセットやソフトウェアのアップグレードが発生した場合、または手動による設定変更が行われた場合、デバイスは影響を受けない可能性があります。

脆弱性を含んでいないことが確認された製品

2010年11月18日より前、または2011年9月19日より後に出荷されたCisco TelePresence System Integrator CシリーズおよびCisco TelePresence EXシリーズデバイスは、この脆弱性の影響を受けません。その他のシスコ製品は、現在のところ影響を受けていません。

詳細

Cisco TelePresence System Integrator CシリーズおよびCisco TelePresence EXシリーズのデバイスは、人と人またはグループのテレプレゼンス通話に、臨場感のあるインタラクティブで魅力的なエクスペリエンスを提供します。

デフォルトのルートアカウント

製造および配布プロセス中に発生したエラーの結果、影響を受ける製品が安全でない設定で配布された可能性があります。この脆弱性は、ライセンス/オプションの設定とテストの後でデバイスをデフォルト設定に戻すことができないことに起因します。

影響を受けるデバイスでは、rootアカウントが有効になっており、既定の既定のパスワードが設定されている可能性があります。このアカウントは、特定のデバッグアクションを実行する必要がある場合にデバイス管理者が有効にすることを目的としており、デフォルトでは無効にする必要があります。

管理者は、次のいずれかの方法を使用して、影響を受けるデバイスの設定を確認できます。

TC4.0または4.1ソフトウェアを実行しているデバイスの場合、管理者は該当デバイスのコマンドラインにadminアカウントでログインし、xstatus systemunit hardwareコマンドを発行することで、該当デバイスのシリアル番号を表示できます。

シリアル番号の表示：

<#root>

ssh admin@203.113.55

```
Welcome to TANDBERG Codec Release TC4.1.0.247017 SW Release
Date: 2011-01-28

OK
```

xstatus SystemUnit Hardware

```
*s SystemUnit Hardware Module SerialNumber: "A1AR12C00024"
*s SystemUnit Hardware Module Identifier: "01"
*s SystemUnit Hardware Module CompatibilityLevel: 0 *s SystemUnit Hardware MainBoard SerialNumber: "F00
*s SystemUnit Hardware MainBoard Identifier: "101540-4 [00]"
*s SystemUnit Hardware VideoBoard SerialNumber: "N/A"
*s SystemUnit Hardware VideoBoard Identifier: "0--1 [N/A]"
*s SystemUnit Hardware AudioBoard SerialNumber: "N/A"
*s SystemUnit Hardware AudioBoard Identifier: "0--1 [N/A]"
*s SystemUnit Hardware BootSoftware: "U-Boot 2010.06-89"
** end
```

rootアカウントの状態の判別：

ソフトウェアリリースTC4.0で導入された機能不具合の結果として、systemtools rootsettings getコマンドは常にoffの値を返します。ソフトウェアリリースTC4.0またはTC4.1を実行しているデバイスのrootアカウントの状態を正確に判別するには、管理者は影響を受けるデバイスにrootとしてSSH接続を開く必要があります。

有効なルートアカウント：

<#root>

ssh root@203.0.113.55

```
[tandberg:~] $
```

無効なルートアカウント：

<#root>

ssh root@203.0.113.55

```
Password:
Password:
Password:

Permission denied (publickey,keyboard-interactive)
```

ソフトウェアリリースTC4.2が稼働しているデバイスの場合、管理者はadminアカウントで該当デバイスのコマンドラインにログインし、次のコマンドのいずれかを発行することで、rootアカウントのシリアル番号またはステータスを表示できます。

シリアル番号の表示：

<#root>

ssh admin@203.0.113.55

```
Welcome to
TANDBERG Codec Release TC4.2.0.260857
SW Release Date: 2011-07-11

OK
```

xstatus SystemUnit Hardware

```
*s SystemUnit Hardware Module SerialNumber: "A1AR12C00024"
*s SystemUnit Hardware Module Identifier: "01"
*s SystemUnit Hardware Module CompatibilityLevel: 0 *s SystemUnit Hardware MainBoard SerialNumber: "F00
*s SystemUnit Hardware MainBoard Identifier: "101540-4 [00]"
*s SystemUnit Hardware VideoBoard SerialNumber: "N/A"
*s SystemUnit Hardware VideoBoard Identifier: "0--1 [N/A]"
*s SystemUnit Hardware AudioBoard SerialNumber: "N/A"
*s SystemUnit Hardware AudioBoard Identifier: "0--1 [N/A]"
*s SystemUnit Hardware BootSoftware: "U-Boot 2010.06-89"
** end

OK
```

ルートアカウントのステータスの表示：

管理者はsystemtools rootsettings getコマンドを発行して、rootアカウントの現在のステータスを取得できます。このコマンドは、次のいずれかの値を返します。

- off（rootユーザが無効であることを示す）
- never（ルートユーザが永続的に無効になっていることを示す）
- serial [password]（rootユーザはシリアルポートでのみ使用可能であることを示します）
- on [password]（rootユーザがすべてのポートで使用可能であることを示します）

<#root>

ssh admin@203.0.113.55

```
Welcome to TANDBERG Codec Release TC4.1.0.247017 SW Release
Date: 2011-01-28

OK
```

```
systemtools rootsettings get
```

```
off
OK
```

コマンドがoffまたはneverを返す場合、rootアカウントは無効になり、デバイスは影響を受けません。

回避策

この脆弱性は、次のいずれかの方法で修正できます。

- 管理者は、adminコマンドラインインターフェイスでsystemtools rootsettings [off|never]コマンドを発行することにより、rootアカウントを手動で無効にできます。
- 管理者は、該当するデバイスを工場出荷時のデフォルトにリセットできます。

Rootユーザの無効化：

<#root>

```
ssh admin@203.0.113.55
```

```
Welcome to
TANDBERG Codec Release TC4.2.0.260857
SW Release Date: 2011-07-11

OK
```

```
systemtools rootsettings off
```

```
OK
Connection to 203.0.113.55 closed by remote host.
```

デバイスを工場出荷時のデフォルトにリセットすると、次のようになります。

- 工場出荷時のデフォルトパスワード

- Session Initiation Protocol(SIP)およびH.323設定を含む、工場出荷時のデフォルト設定
- ローカルの電話帳
- すべてのログ
- DHCP情報

デバイスにインストールされているソフトウェアリリースとオプションキーはそのまま残ります。

管理者は、次の手順を使用して工場出荷時の初期状態にリセットできます。

コマンドラインファクトリリセット（C20、C40、C60、C90、EX60、EX90コーデック）:

<#root>

ssh admin@203.0.113.55

```
Welcome to
TANDBERG Codec Release TC4.2.0.260857
SW Release Date: 2011-07-11

OK
```

xCommand systemunit FactoryReset Confirm: Yes

その後、デバイスがリブートします。完了すると、デバイスは工場出荷時のデフォルトにリセットされ、使用する前に追加の設定が必要になります。

一部のCisco TelePresence System Integrator CシリーズおよびCisco TelePresence EXシリーズデバイスは、物理デバイス上で一連の操作を実行することにより、工場出荷時のデフォルトに戻すこともできます。この方法を使用するには、デバイス操作ガイドを参照してください。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレード 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機器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。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco 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やその公表は確認しておりません。

この脆弱性は、該当デバイスの内部監査中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111109-telepresence-c-ex-series

改訂履歴

リビジョン 1.2	2011-November-15	コマンド例を更新して説明テキストと一致させます。
リビジョン 1.1	2011年11月9日	2011年2月2日のセキュリティアドバイザリへのリンクを修正。
リビジョン 1.0	2011年11月9日	初回公開リリース

利用規約

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も示唆するものではありません。 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、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。