# Multiple Vulnerabilities in Cisco TelePresence TC and TE Software

Advisory ID: cisco-sa-20130619-tpc

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130619-tpc/

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 June 19 16:00 UTC (GMT)

## 目次



## 要約


Cisco TelePresence TC および TE ソフトウェアには Session Initiation Protocol（SIP; セッション開始プロトコル）の実装面において 2 つの脆弱性があり、認証されていないリモートの攻撃者が DoS（サービス拒否）状態を引き起こす可能性があります。
さらに、Cisco TelePresence TC ソフトウェアには近接 *root* アクセスの脆弱性が存在するため、該当システムと同一の物理または論理レイヤ 2 ネットワーク上の攻撃者が、認証されていない *root* シェルを取得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 TelePresence TC および TE ソフトウェアにおける SIP の DoS 脆弱性の影響を軽減する回避策があります。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-20130619-tpc/


## 該当製品

### 脆弱性が認められる製品

Cisco TelePresence TC および TE ソフトウェアの脆弱性が存在するバージョンを稼働している

次の製品は、SIP の DoS 脆弱性による影響を受けます。

- Cisco TelePresence MX シリーズ
- Cisco TelePresence System EX シリーズ
- Cisco TelePresence Integrator C シリーズ
- Cisco TelePresence Profiles シリーズ
- Cisco TelePresence Quick Set シリーズ
- Cisco IP Video Phone E20

Cisco TelePresence TC ソフトウェアを稼働している次の製品は、Cisco TelePresence TC ソフトウェアにおける近接 root アクセスの脆弱性による影響を受けます。

- Cisco TelePresence MX シリーズ
- Cisco TelePresence System EX シリーズ
- Cisco TelePresence Integrator C シリーズ
- Cisco TelePresence Profiles シリーズ
- Cisco TelePresence Quick Set シリーズ

注：Cisco TelePresence TE ソフトウェアは、Cisco TelePresence TC ソフトウェアにおける近接 root アクセスの脆弱性による影響を受けません。

## 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 TelePresence TC および TE ソフトウェアにおける SIP の DoS 脆弱性

Cisco TelePresence TC および TE ソフトウェアには Session Initiation Protocol（SIP; セッション開始プロトコル）の実装面に 2 つの異なる脆弱性があり、認証されていないリモートの攻撃者によって DoS 状態が引き起こされる可能性があります。
いずれの脆弱性も、該当システムに送信された巧妙に細工された SIP パケットの検証が不十分なことに起因します。攻撃者は巧妙に細工された SIP パケットを該当システムに送信することで、両方の脆弱性を不正利用する可能性があります。

1 つ目の脆弱性は、Cisco Bug ID CSCue01743（ 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-2013-3377 が割り当てられています。
この脆弱性の不正利用に成功した場合、該当システムのリロードが引き起こされることがあります。

2 つ目の脆弱性は、Cisco Bug ID CSCuf89557（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2013-3378 が割り当てられています。
この脆弱性の不正利用に成功した場合、該当システムが一定期間にわたり応答不能になる可能性があります。この脆弱性が繰り返し悪用されると、持続的なサービス拒否状態に陥る可能性があります。

### Cisco TelePresence TC ソフトウェアにおける近接 root アクセスの脆弱性

ファイアウォール ルールの実装面における脆弱性により、認証されていない、近接した攻撃者が該当システムの *root* シェル アクセスを取得する可能性があります。

この脆弱性は、ファイアウォール ルール内で許可されたホストの実装が不適切であることに起因します。攻撃者は該当システムの管理 IP アドレスに接続して、この脆弱性を不正利用する可能性

があります。攻撃者がこの脆弱性を不正利用するには、論理的または物理的に近接している必要があります。不正利用によって攻撃者がシェルへの *root* アクセスを取得する可能性があります。

この脆弱性は、Cisco Bug ID CSCts37781（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2013-3379 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/

| CSCue01743 - Cisco TelePresence TC and TE Software SIP Denial of Service Vulnerability<br>Calculate the environmental score of | | | | | |
|---|---|---|---|---|---|
| CVSS Base Score - **7.8** | | | | | |
| Access Vector | Access Complexity | Authentication | Confidentiality Impact | Integrity Impact | Availability Impact |
| Network | Low | None | None | None | Complete |
| CVSS Temporal Score - **6.4** | | | | | |
| Exploitability | | Remediation Level | | Report Confidence | |
| Functional | | Official-Fix | | Confirmed | |

| CSCuf89557 - Cisco TelePresence TC and TE Software SIP Denial of Service Vulnerability<br>Calculate the environmental score of |
|---|

| CVSS Base Score - 7.8 | | | | | |
|---|---|---|---|---|---|
| Access Vector | Access Complexity | Authentication | Confidentiality Impact | Integrity Impact | Availability Impact |
| Network | Low | None | None | None | Complete |
| CVSS Temporal Score - 6.4 | | | | | |
| Exploitability | | Remediation Level | | Report Confidence | |
| Functional | | Official-Fix | | Confirmed | |

| CSCts37781 - Cisco TelePresence TC Software Adjacent root Access Vulnerability<br>Calculate the environmental score of | | | | | |
|---|---|---|---|---|---|
| CVSS Base Score - 8.3 | | | | | |
| Access Vector | Access Complexity | Authentication | Confidentiality Impact | Integrity Impact | Availability Impact |
| Adjacent Network | Low | None | Complete | Complete | Complete |
| CVSS Temporal Score - 6.9 | | | | | |
| Exploitability | | Remediation Level | | Report Confidence | |
| Functional | | Official-Fix | | Confirmed | |

## 影響

Cisco TelePresence TC および TE ソフトウェアにおける SIP の DoS 脆弱性の不正利用に成功すると、システムの応答不能またはリロードが引き起こされる可能性があります。

Cisco TelePresence TC ソフトウェアにおける近接 root アクセスの脆弱性の不正利用に成功すると、 該当システムと同一の物理または論理レイヤ 2 ネットワーク上の攻撃者が認証されていない *root* シェルを取得でき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

### Cisco TelePresence TC および TE ソフトウェアにおける SIP の DoS 脆弱性

次の表に、Cisco bug ID CSCue01743 および CVE ID CVE-2013-3377 で特定された Cisco TelePresence TC および TE ソフトウェアの脆弱性に対する修正を含むリリースを各該当製品別に記載します。

| Products | Affected Releases | Resolved In |
|---|---|---|
| Cisco TelePresence MX Series | TC5.x and earlier | TC5.1.7 or later |
| Cisco TelePresence System EX Series | TC5.x and earlier | TC5.1.7 or later |
| Cisco TelePresence System EX Series | TE6.0 | TC6.1 or later |
| Cisco TelePresence Integrator C Series | TC5.x and earlier | TC5.1.7 or later |
| Cisco TelePresence Profiles Series | TC5.x and earlier | TC5.1.7 or later |
| Cisco TelePresence Quick Set Series | TC5.x and earlier | TC5.1.7 or later |
| Cisco IP Video Phone E20 | TE4.x and earlier | TE4.1.3 |

次の表に、Cisco bug ID CSCuf89557 および CVE ID CVE-2013-3378 で特定された脆弱性への Cisco TelePresence TC および TE ソフトウェア向けの修正を含むリリースに関する情報を各該当製品別に記載します。

| Products | Affected Releases | Resolved In |
|---|---|---|
| Cisco TelePresence MX Series | TC6.x and earlier | TC6.1 or later |
| Cisco TelePresence System EX Series | TC6.x and earlier | TC6.1 or later |
| Cisco TelePresence System EX Series | TE6.0 | TC6.1 or later |
| Cisco TelePresence Integrator C Series | TC6.x and earlier | TC6.1 or later |
| Cisco TelePresence Profiles Series | TC6.x and earlier | TC6.1 or later |
| Cisco TelePresence Quick Set Series | TC6.x and earlier | TC6.1 or later |
| Cisco IP Video Phone E20 | TE4.x and earlier | TE4.1.3 |

### Cisco TelePresence TC ソフトウェアにおける近接 root アクセスの脆弱性

次の表に、Cisco TelePresence TC ソフトウェアにおける近接 root アクセスの脆弱性に対する修正を含むリリースについての情報を各該当製品別に記載します。

| Products | Affected Releases | Resolved In |
|---|---|---|
| Cisco TelePresence MX Series | TC4.1 and earlier | TC4.2 or later |
| Cisco TelePresence System EX Series | TC4.1 and earlier | TC4.2 or later |
| Cisco TelePresence Integrator C Series | TC4.1 and earlier | TC4.2 or later |
| Cisco TelePresence Profiles Series | TC4.1 and earlier | TC4.2 or later |
| Cisco TelePresence Quick Set Series | TC4.1 and earlier | TC4.2 or later |

### 推奨リリース

次の表に、このアドバイザリで説明したすべての脆弱性を解決する Cisco TelePresence TC および TE ソフトウェアの推奨リリースに関する情報を記載します。

| Products | Recommended Release |
|---|---|
| Cisco TelePresence MX Series | TC6.1 or later |

| | |
|---|---|
| Cisco TelePresence System EX Series | TC6.1 or later |
| Cisco TelePresence System EX Series | TC6.1 or later |
| Cisco Telepresence Integrator C Series | TC6.1 or later |
| Cisco TelePresence Profiles Series | TC6.1 or later |
| Cisco TelePresence Quick Set Series | TC6.1 or later |
| Cisco IP Video Phone E20 | TE4.1.3 |

**注**：Cisco IP Video Phone E20 向けの Cisco TelePresence TE ソフトウェア バージョン 4.1.3 は 2013 年 6 月 30 日から提供される予定です。

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

**Cisco TelePresence TC および TE ソフトウェアにおける SIP の DoS 脆弱性**

SIP を使用していない場合、SIP サービスを無効にすることでこれら脆弱性を回避することができます。次の xCommand を実行して **NetworkServices** SIP Mode を Off に設定します。

```
xConfiguration NetworkServices SIP Mode: Off
```

または、管理者が Web インターフェイスを使用して SIP サービスを無効にすることもできます。[Configuration] > [Advanced Configuration] > [Network Services] を開き、SIP モードを Off に設定します。

**Cisco TelePresence TC ソフトウェアにおける近接 root アクセスの脆弱性**

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 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。

Cisco bug ID CSCue01743 および CVE ID CVE-2013-3377 で特定された脆弱性は、シスコ内部でのテストによって発見されました。

Cisco bug ID CSCuf89557 および CVE ID CVE-2013-3377 で特定された脆弱性は、nSense の Knud 氏からシスコにご報告いただきました。

Cisco TelePresence TC ソフトウェアにおける近接 root アクセスの脆弱性は、シスコ内部でのテストによって発見されました。

## 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-20130619-tpc/

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-June-19 | 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。