Cisco TelePresence TCおよびTEソフトウェアの複数の脆弱性

High

アドバイザリーID : cisco-sa-20130619-tpc
初公開日 : 2013-06-19 16:00
バージョン 1.0 : Final
CVSSスコア : 8.3
回避策 : No Workarounds available
Cisco バグ ID : CSCue01743 CSCts37781 CSCuf89557

CVE-2013-3379
CVE-2013-3377
CVE-2013-3378

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 TCおよびTEソフトウェアには、Session Initiation Protocol(SIP)の実装に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によってサービス妨害(DoS)状態が引き起こされる可能性があります。
さらに、Cisco TelePresence TCソフトウェアには、隣接する ルートアクセスの脆弱性があり、影響を受けるシステムと同じ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ルート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処するソフトウェアアップデートをリリースしています。Cisco TelePresence TCおよびTEソフトウェアのSIPに関するDoS脆弱性を軽減する回避策があります。このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130619-tpc

該当製品

脆弱性のある製品

脆弱性のあるバージョンのCisco TelePresence TCおよびTEソフトウェアを実行している次の製品は、SIP DoS脆弱性の影響を受けます。

- Cisco TelePresence MX Series
- Cisco TelePresence System EX シリーズ
- Cisco TelePresence Integrator C Series
- Cisco TelePresence Profilesシリーズ実行中（自動）

- Cisco TelePresence Quick Setシリーズ
- Cisco IP Video Phone E20

Cisco TelePresence TCソフトウェアを実行している次の製品は、Cisco TelePresence TCソフトウェアの隣接ルートアクセスの脆弱性の影響を受けます

- Cisco TelePresence MX Series
- Cisco TelePresence System EX シリーズ
- Cisco TelePresence Integrator C Series
- 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ソフトウェアの隣接ルートアクセスの脆弱性の影響を受けません

脆弱性を含んでいないことが確認された製品

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

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

Cisco TelePresence TCおよびTEソフトウェアには、Session Initiation Protocol(SIP)の実装に2つの異なる脆弱性が存在します。認証されていないリモートの攻撃者によってサービス妨害(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であることに起因します。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。

最初の脆弱性は、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すると、該当システムのリロードが引き起こされる可能性があります。

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すると、影響を受けるシステムが一定時間応答しなく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隣接ルートアクセスの脆弱性

ファイアウォールルールの実装における脆弱性により、認証されていない隣接する攻撃者が、該当システムへの 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で許可されたホストの不適切な実装に起因します。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。攻撃者がこの脆弱性を不正利用するには、論理的または物理的に隣接している必要があります。この不正利用により、攻撃者はシェルへの rootアクセス権を取得でき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。

回避策

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

SIPを使用していない場合は、SIPサービスを無効にしてこれらの脆弱性に対する回避策を実行できます。次のxCommandを発行して、 NetworkServices SIPモードをOffに設定します。

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

または、管理者はWebインターフェイスを使用してSIPサービスを無効にできます。Configuration > Advanced Configuration > Network Servicesの順に移動し、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隣接ルートアクセスの脆弱性

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

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

次の表に、Cisco Bug ID CSCue01743およびCVE ID CVE-2013-3377で特定された脆弱性に対するCisco TelePresence TCおよびTEソフトウェアの修正済みリリースを、該当製品ごとに示します。

製品	該当するリリース	解決されたバージョン
Cisco TelePresence MX Series	TC5.x以前	TC5.1.7以降
Cisco TelePresence System EX シリーズ	TC5.x以前	TC5.1.7以降

Cisco TelePresence System EX シリーズ	TE6.0	TC6.1以降
Cisco TelePresence Integrator C Series	TC5.x以前	TC5.1.7以降
Cisco TelePresence Profilesシリーズ	TC5.x以前	TC5.1.7以降
Cisco TelePresence Quick Setシリーズ	TC5.x以前	TC5.1.7以降
Cisco IP Video Phone E20	TE4.x以前	TE4.1.3

次の表に、Cisco TelePresence TCおよびTEソフトウェアの修正済みリリースに関する情報を示します。これらの情報は、影響を受ける各製品のCisco Bug ID CSCuf89557およびCVE ID CVE-2013-3378で特定されている脆弱性を参照しています。

製品	該当するリリース	解決されたバージョン
Cisco TelePresence MX Series	TC6.x以前	TC6.1以降
Cisco TelePresence System EX シリーズ	TC6.x以前	TC6.1以降
Cisco TelePresence System EX シリーズ	TE6.0	TC6.1以降
Cisco TelePresence Integrator C Series	TC6.x以前	TC6.1以降
Cisco TelePresence Profilesシリーズ	TC6.x以前	TC6.1以降
Cisco TelePresence Quick Setシリーズ	TC6.x以前	TC6.1以降
Cisco IP Video Phone E20	TE4.x以前	TE4.1.3

Cisco TelePresence TCソフトウェアにおける隣接ルートアクセスの脆弱性

次の表に、Cisco TelePresence TCソフトウェアの隣接ルートアクセスの脆弱性に対する修正済みリリースに関する情報を、該当製品ごとに示します。

製品	該当するリリース	解決されたバージョン
Cisco TelePresence MX Series	TC4.1以前	TC4.2以降
Cisco TelePresence System EX シリーズ	TC4.1以前	TC4.2以降
Cisco TelePresence Integrator C Series	TC4.1以前	TC4.2以降
Cisco TelePresence Profilesシリーズ	TC4.1以前	TC4.2以降
Cisco TelePresence Quick Setシリーズ	TC4.1以前	TC4.2以降

推奨リリース

次の表に、このアドバイザリに記載されている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示します。

製品	推奨リリース
Cisco TelePresence MX Series	TC6.1以降
Cisco TelePresence System EX シリーズ	TC6.1以降
Cisco TelePresence System EX シリーズ	TC6.1以降
Cisco Telepresence Integrator C シリーズ	TC6.1以降
Cisco TelePresence Profilesシリーズ	TC6.1以降
Cisco TelePresence Quick Setシリーズ	TC6.1以降
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日から利用可能になります。

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 and Responses アーカイブや後続のアドバイザリを参照して、侵害を受ける可能性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。

推奨事項

$propertyAndFields.get("recommendations")

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エクスプロイト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、内部テストで発見されたものです。

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氏によってシスコに報告されました。

Cisco TelePresence TCソフトウェアの隣接ルートアクセスの脆弱性は、内部テストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130619-tpc

改訂履歴

リビジョン 1.0	2013年6月19日	初版リリース

利用規約

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。