Cisco Unified IP Phone Local Kernel System Call Input Validation Vulnerability

Advisory ID: cisco-sa-20130109-uipphone

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130109-uipphone

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 January 9 16:00 UTC (GMT)

目次

要約

Cisco Unified IP Phones 7900 シリーズ バージョン 9.3(1)SR1 以前には、任意のコードが実行される脆弱性が存在します。これにより、ローカルの攻撃者が特権権限を使用してコードを実行したり、任意のメモリを改ざんできる可能性があります。

この脆弱性は、ユーザスペースで稼働しているアプリケーションからカーネル システム コールに送られる入力に対する検証が適切に行われないことに起因します。攻撃者は、物理アクセス、または SSH を使用した認証アクセスを使用してデバイスへのローカル アクセスを取得し、この問題の不正利用を目的として設計され、かつ攻撃者によって制御されるバイナリを実行して、この問題を不正利用する可能性があります。攻撃は非特権コンテキストから行われる可能性があります。

この問題は Ang Cui 氏によって最初に Cisco Product Security Incident Response Team（PSIRT）に報告されました。Cisco PSIRT は 2012 年 11 月 6 日に、この問題を Cisco bug ID CSCuc83860（ 登録ユーザ専用 ）のリリース ノート付属文書で公開しました。その後、Cui 氏は複数の公開会議で講演し、その中で、改ざんされリスニング デバイスとして使用されて

いるデバイスの公開デモンストレーションを行いました。

影響を受けるデバイスの攻撃個所を削減する緩和策があります。詳細情報は、本アドバイザリの「詳細」セクションと、付属ドキュメント『Cisco Applied Mitigation Bulletin』（AMB）を参照してください。

このアドバイザリは、次のリンク先で確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130109-uipphone

該当製品

この脆弱性は、Cisco Unified IP Phone 7900 シリーズ（TNP 電話とも呼ばれる）に影響を与えます。

脆弱性が存在する製品

次の Cisco Unified IP Phones 7900 シリーズ デバイスが、このアドバイザリに記載されている脆弱性の影響を受けます。

- Cisco Unified IP Phone 7906
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7975G

脆弱性が存在しない製品

次の Cisco Unified IP Phones 7900 シリーズ デバイスは、このアドバイザリに記載されている脆弱性の影響を受けません。

- Cisco Unified IP Phone 7902G
- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7910G
- Cisco Unified IP Phone 7912G
- Cisco Unified IP Phone 7940
- Cisco Unified IP Phone 7960
- Cisco Unified IP Phone 7985G
- Cisco Unified Wireless IP Phone 7920 バージョン 1/2/3
- Cisco Unified Wireless IP Phone 7921G
- Cisco Unified Wireless IP Phone 7925G
- Cisco Unified Wireless IP Phone 7925G-EX
- Cisco Unified Wireless IP Phone 7926G
- Cisco Unified IP Conference Station 7935

- Cisco Unified IP Conference Station 7936
- Cisco Unified IP Conference Station 7937G

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 Unified IP Phone 7900 シリーズの複数のモデルには、入力検証に関する脆弱性が存在します。これにより、ローカルの認証された攻撃者がデバイス内メモリの任意の領域を操作できる可能性があります。これは、カーネル システム コールに送られるユーザ提供のパラメータに対して検証が適切に行われないことに起因します。また、攻撃者がデバイスへのローカル アクセスを実行するための複数のアクセス ベクトルが確認されています。それらは、デバイス背面の AUX ポートから物理的にアクセスすること、または SSH で最初にデバイスの認証を受けてリモートからアクセスすることです。Cisco Unified Communications Manager（CallManager）によってデバイスのプロビジョニングが行われると、リモート アクセスはデフォルトで無効になります。

公開デモンストレーション

この問題は、複数の場所で公開デモンストレーションが行われています。各デモンストレーションで使用されているデバイスは、該当する Cisco Unified IP Phone ソフトウェア バージョンを実行している、プロビジョニングされていない電話だと思われます。デモンストレーションでは物理的な攻撃ベクトル、つまりローカル シリアル ポート経由で電話に侵入して、改ざんしたバイナリをデバイスに配置し、それを使用してカーネル メモリの任意の領域を操作するという不正利用を行っています。

デモンストレーションでは、オンフックの状態（受話器をクレードルに置いた状態）で受話器のマイクがオンにされています。TNP デバイスの高利得エリア マイクロフォンはスピーカーフォンのアクティブ インジケータに電気的に接続されており、ソフトウェア操作によってバイパスすることはできません。79x1 シリーズ デバイスでは、受話器のマイクロフォンはソフトウェアおよびオーディオ コーデックの汎用入出力（GPIO）チャネルによって制御されるため、マイクロフォンがオンにされ受話器のディスプレイ インジケータがバイパスされる可能性があります。

79x2 および 79x5 シリーズ デバイスは、受話器のマイクロフォンをオフフック スイッチに電気的に接続するという設計でさらなる保護を提供しており、マイクロフォンが何の表示もなくオンにされることはありません。

予想されるリモート攻撃

物理的な攻撃ベクトルに加え、Cisco Unified IP Phone の特定の挙動を利用した複数のネットワークベースの攻撃が予想されます。これまでのところ、攻撃は TFTP を使用した不正利用がベースとなっています。TFTP は UDP で運用される、安全ではない転送プロトコルであり、スプーフィング攻撃を受けやすくなっています。シスコは、TFTP が安全でないことを認識しており、Cisco Unified Call Manager バージョン 5.0 以降では、TFTP で転送される電話設定ファイルを管理者が暗号化できるようにすることで安全を保てるようにしています。さらに、バージョン 8.0(1) 以降の全リリースでは、Secure By Default ポリシーを導入しています。これらのリリースではデフォルトでデバイスの設定ファイルに署名し、電話の SSH と Web デーモンの両方を無効にします。デバイス設定ファイルの署名と暗号化によって、攻撃者が TFTP サーバまたはサーバの応答をスプーフィングしてこれらのファイルを改ざんすることや置き換えたりすることを防止します。デバイス設定ファイルは、デバイスに使用される前にその暗号署名が検証されるため、不正利用を防止することができます。

これらのデフォルトの保護に加え、シスコはすべての音声ネットワーク展開向けの包括的な設計

ガイドを提供しています。ガイドには、スプーフィングされたトラフィックが音声ネットワーク上で送信されるのを防止する方法や、一般のネットワーク トラフィックと音声トラフィックの隔離など、中間デバイスとエッジ デバイスに関して推奨されるセキュリティ機能構成が含まれています。Cisco Unified Communications Manager バージョン 9.0 のセキュリティ情報は、次のリンク先で確認できます。
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/9x/security.html

ネットワーク、デバイス、設定に基づいた数々の緩和策はあるものの、該当するデバイスへの物理攻撃ベクトルに対する緩和策はありません。これに関してシスコは段階的な修正アプローチを実施します。このアドバイザリに記載された脆弱性について、既知の攻撃ベクトルを緩和する中間的な Engineering Special ソフトウェアを、該当するデバイス向けにリリースする予定です。このソフトウェア リリースは、提供開始後、Cisco Technical Assistance Center（TAC）より請求に応じて提供されます。その後、その他の強化点が Cisco.com の Service Release に掲載されます。

これら 2 つのリリースによって、管理者は音声環境の安全性を充分に確保できるはずですが、シスコはこの脆弱性の根本原因の長期的な修正の提供にも取り組みます。今後数ヵ月にわたり、シスコは 7900 シリーズのファームウェアを一部書き換え、根本原因に対処するとともに、該当するデバイスのネットワーク セキュリティおよび物理的セキュリティの両方を改善していく予定です。シスコは、安全性を最大限に高めた IP テレフォニー デバイスを提供するとともに、お客様の既存のインフラストラクチャに対する投資を継続的に保護することを目標としています。

この脆弱性は、Cisco Bug ID CSCuc83860（ 登録ユーザのみ ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2012-5445 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組織の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、自身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 計算ツールを次のリンクで提供しています。

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

CSCuc83860 Calculate the environmental score of

CVSS Base Score - 6.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Local	Low	Single	Complete	Complete	Complete
CVSS Temporal Score - 5.8					
Exploitability		Remediation Level		Report Confidence	
Functional		Temporary-Fix		Confirmed	

影響

この脆弱性の不正利用に成功した場合、ローカルの攻撃者はカーネル領域を含むシステム メモリの任意の領域を操作できる可能性があります。成功した場合、攻撃者は既存のコードの動作を改ざんしたり、攻撃者によって制御できるコードを特権権限で実行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

シスコは現時点でまだ修正済みソフトウェアをリリースしていません。シスコは、このアドバイザリに記載された脆弱性に対する既知の攻撃ベクトルを回避する Engineering Special ソフトウェアを、1 月 21 日の週にリリースする予定です。

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 and Responses アーカイブや、本アドバイザリ以降に公開のアドバイザリを参照して、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

管理者には、次の『Applied Mitigation Bulletin』に記載された緩和策を読み、実行することが推奨されます。Cisco Unified IP Phone がシスコのインフラストラクチャで導入されていない場合、管理者には少なくとも、暗号化された構成の導入を検討すること、および SSH が無効にされていることを確約することが推奨されます。Cisco Unified Communications Manager バージョン 8.0(1) 以降の設定ファイルは、すべての該当する Cisco Unified IP Phone 7900 シリーズ デバイスに対してデフォルトで署名されています。

ネットワーク内のシスコ デバイスに適用可能なその他の緩和策については、次のリンクにあるこのアドバイザリの付属ドキュメント、『Identifying and Mitigating Exploitation of the Cisco Unified IP Phone Local Kernel System Call Input Validation Vulnerability』で参照できます。
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=27763

修正済みソフトウェアの入手

シスコは現時点でまだ修正済みソフトウェアをリリースしていません。シスコは、このアドバイザリに記載された脆弱性に対する既知の攻撃ベクトルを回避する Engineering Special ソフトウェアを、1 月 21 日の週にリリースする予定です。

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を入手することができます。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、適切な処置について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。影響製品およびリリース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または修正が最適であるか、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。

- +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 を通して無償アップグレードをお求めください。

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、シスコ ワールドワイドお問い合わせ先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いかなる不正利用事例も確認しておりません。

この脆弱性は、コロンビア大学の Ang Cui 氏によってシスコに報告されました。

この通知のステータス: INTERIM

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。新しい情報が入り次第、このドキュメントは更新される予定です。

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-20130109-uipphone

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電子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

このアドバイザリに関する今後の更新があれば、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。このアドバイザリの URL で更新をご確認いただくことができます。

更新履歴

Revision 1.0	2013-January-09	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、Cisco.com 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 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。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。