

# Cisco Security Advisory: Multiple Vulnerabilities in Cisco Unified IP Phones 7900 Series

Advisory ID: cisco-sa-20110601-phone

<http://www.cisco.com/warp/public/707/cisco-sa-20110601-phone.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 June 1 1600 UTC (GMT)

## 目次

- [要約](#)
- [該当製品](#)
- [詳細](#)
- [脆弱性スコア詳細](#)
- [影響](#)
- [ソフトウェア バージョンおよび修正](#)
- [回避策](#)
- [修正済みソフトウェアの入手](#)
- [不正利用事例と公式発表](#)
- [この通知のステータス: FINAL](#)
- [情報配信](#)
- [更新履歴](#)
- [シスコ セキュリティ手順](#)

## 要約

Cisco Unified IP Phone 7900 シリーズ デバイス ( TNP 電話 ) は、3 件の脆弱性による影響を受けます。これらの脆弱性により、攻撃者は権限の昇格、電話設定の変更、機密情報の開示、署名のないソフトウェアの読み込みが可能になることがあります。これら 3 件の脆弱性は、権限昇格の脆弱性 2 件と、署名バイパスの脆弱性 1 件に分類されます。

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。この脆弱性を軽減する回避策はありません。

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-20110601-phone.shtml>

## 該当製品

Cisco Unified IP Phone 7900 シリーズ デバイス ( TNP 電話 ) のみが該当します。

## 脆弱性が存在する製品

次の Cisco Unified IP Phone デバイ스에脆弱性が存在します。

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

次のモデルはサポート終了 ( EOL ) となっています ( ハードウェアのみ ) 。

- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7906

利用可能な製品アップグレードおよび交換オプションを確認するには、次のリンクを参照してください。

[http://www.cisco.com/en/US/products/hw/phones/ps379/prod\\_eol\\_notices\\_list.html](http://www.cisco.com/en/US/products/hw/phones/ps379/prod_eol_notices_list.html)

## 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

Cisco Unified IP Phone 7900 シリーズ デバイスは権限昇格の脆弱性 2 件と、署名バイパスの脆弱性 1 件の影響を受けます。次のセクションでは、このセキュリティ アドバイザリに記載された各脆弱性の詳細を説明します。

## 権限昇格の脆弱性

Cisco Unified IP Phone 7900 シリーズ デバイスは権限昇格の脆弱性 2 件の影響を受けます。これにより、認証された攻撃者によって電話の不正な設定変更や、機密事項を含む情報の取得が可能になることがあります。

これらの脆弱性は Cisco Bug ID [CSCtf07426](#) ( [登録ユーザのみ](#) ) および [CSCtn65815](#) ( [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-2011-1602 および CVE-2011-1603 がそれぞれ割り当てられています。

## 署名照合バイパスの脆弱性

Cisco Unified IP Phone 7900 シリーズ デバイスは、署名照合バイパスの脆弱性による影響を受けます。これにより、認証された攻撃者が署名照合を経ずにソフトウェア イメージを読み込むことが可能になることがあります。

この脆弱性は Cisco Bug ID [CSCtn65962](#) ( [登録ユーザのみ](#) ) として文書化され、CVE ID として CVE-2011-1637 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>

<b>CSCtf07426 - Privilege Escalation with "su" utility</b>					
<b>Calculate the environmental score of</b>					
CVSS Base Score - 6.6					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Local	Medium	Single	Complete	Complete	Complete
CVSS Temporal Score - 5.5					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	
<b>CSCtn65815 - Privilege Escalation in IP Phones</b>					
<b>Calculate the environmental score of</b>					
CVSS Base Score - 6.6					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Local	Medium	Single	Complete	Complete	Complete
CVSS Temporal Score - 5.5					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	
<b>CSCtn65962 - Phones Permits the Installation of Unsigned Code</b>					
<b>Calculate the environmental score of</b>					
CVSS Base Score - 1.5					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Local	Medium	Single	Partial	None	None
CVSS Temporal Score - 1.2					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

## 影響

権限昇格の脆弱性（2件）の不正利用に成功すると、認証された攻撃者が電話の設定を変更した

り、システム情報を取得したりすることが可能になります。

署名照合バイパスの脆弱性の不正利用に成功すると、認証された攻撃者が署名照合を経ずにソフトウェアイメージを読み込み、実行することが可能になります。

## 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。

Vulnerability	First Fixed Release
CSCtf07426 - Privilege Escalation with "su" utility	9.0.3
CSCtn65815 - Privilege Escalation in IP Phones	9.2.1
CSCtn65962 - Phones Permits the Installation of Unsigned Code	9.2.1

## 回避策

これらの脆弱性を軽減する回避策はありません。注：これらの脆弱性はすべて攻撃者が認証されている必要があります。

## 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、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 チャン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、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、その他の TAC の連絡先情報については、 [http://www.cisco.com/en/US/support/tsd\\_cisco\\_worldwide\\_contacts.html](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](#)

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とその公表は確認しておりません。

これらの脆弱性は Qualcomm の Matt Duggan 氏によって発見され、シスコに報告されました。

## [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識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-20110601-phone.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](mailto:cust-security-announce@cisco.com)
- [first-bulletins@lists.first.org](mailto:first-bulletins@lists.first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto: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-June-01	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](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。