# Multiple Vulnerabilities in Cisco Unified Customer Voice Portal Software

Advisory ID: cisco-sa-20130508-cvp

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130508-cvp/

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 1.1

For Public Release 2013 May 10 19:30 UTC (GMT)

For Public Release 2013 May 8 16:00 UTC (GMT)

## 目次



## 要約


Cisco Unified Customer Voice Portal（Unified CVP）ソフトウェアには複数の脆弱性が存在します。Cisco Unified CVP のさまざまなコンポーネントがこの影響を受けます。脆弱性に関する詳細情報は、「詳細」セクションを参照してください。これらの脆弱性は個別に不正利用される可能性があります。また、同一のデバイスで 2 つ以上の脆弱性が不正利用され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。この中のいくつかの脆弱性には影響を軽減する回避策が存在します。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-20130508-cvp/


## 該当製品

## 脆弱性が認められる製品

バージョン 9.0.1 ES 11 より前の Cisco Unified CVP ソフトウェアが影響を受けます。

## 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 Unified CVP は、お客様が必要な情報をコンタクト センターから取得することを可能にする Interactive Voice Response（IVR）システムです。

**Cisco Unified Customer Voice Portal ソフトウェアの SIP INVITE パケットの脆弱性**
Cisco Unified CVP の CallServer コンポーネントに存在する不正な SIP INVITE の脆弱性により、認証されていないリモートの攻撃者がシステムの新規コール受付不能を引き起こす可能性があります。
この脆弱性は、不正な SIP INVITE パケットの不適切な処理に起因します。攻撃者は不正な SIP INVITE パケットを Cisco Unified CVP サーバに送信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。
この脆弱性は、Cisco Bug ID CSCua65148（登録ユーザ専用）として文書化され、CVE ID として CVE-2013-1220 が割り当てられています。

**Cisco Unified Customer Voice Portal ソフトウェアの Tomcat Web アプリケーションの脆弱性**
Cisco Unified CVP の Tomcat Web 管理コンポーネントにおける Tomcat Web アプリケーションの脆弱性により、認証されていないリモートの攻撃者が権限を昇格し、管理者アクセス権を取得する可能性があります。
この脆弱性は、Tomcat コンポーネントの不適切な構成に起因します。
この脆弱性は、Cisco Bug ID CSCub38384（登録ユーザ専用）として文書化され、CVE ID として CVE-2013-1221 が割り当てられています。

**Cisco Unified Customer Voice Portal ソフトウェアの Tomcat 構成の脆弱性**
Cisco Unified CVP の Tomcat Web 管理コンポーネントにおける Tomcat Web アプリケーションの脆弱性により、認証されていないリモートの攻撃者が、許可されていないユーザから提供された Web アプリケーションを実行する可能性があります。
この脆弱性は、Tomcat コンポーネントの不適切な構成に起因します。
この脆弱性は、Cisco Bug ID CSCub38379（登録ユーザ専用）として文書化され、CVE ID として CVE-2013-1222 が割り当てられています。

**Cisco Unified Customer Voice Portal ソフトウェア の ファイル アクセスの脆弱性**
Cisco Unified CVP のログ ビューアに存在するファイル アクセスの脆弱性により、認証されていないリモートの攻撃者が任意のシステム ファイルを閲覧する可能性があります。
この脆弱性は、不正確なパラメータ チェックに起因します。攻撃者は細工したリクエストをログ ビューアに送信することで、この脆弱性を不正利用する可能性があります。
この脆弱性は、Cisco Bug ID CSCub38372（登録ユーザ専用）として文書化され、CVE ID として CVE-2013-1223 が割り当てられています。

**Cisco Unified Customer Voice Portal ソフトウェアのパス トラバーサルの脆弱性**
Cisco Unified CVP のリソース マネージャ コンポーネントに存在するパス トラバーサルの脆弱性により、認証されていないリモートの攻撃者がシステム ファイルを上書きする可能性があります。
この脆弱性は、不正確なパラメータ チェックに起因します。攻撃者は細工したリクエストをリソース マネージャに送信することで、この脆弱性を不正利用する可能性があります。

この脆弱性は、Cisco Bug ID CSCub38369（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2013-1224 が割り当てられています。

**Cisco Unified Customer Voice Portal ソフトウェアの XML エンティティ拡張の脆弱性**
Cisco Unified CVP に存在するファイル アクセスの脆弱性により、認証されていないリモートの攻撃者が任意のシステム ファイルを閲覧する可能性があります。
この脆弱性は、XML エンティティ拡張のチェックが行われないことに起因します。攻撃者は細工したリクエストをリソース マネージャに送信することで、この脆弱性を不正利用する可能性があります。
この脆弱性は、Cisco Bug ID CSCub38366（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2013-1225 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/

| **CSCua65148 - Cisco Unified Customer Voice Portal Software SIP INVITE Packet Vulnerability 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 | |

| CSCub38384 - Cisco Unified Customer Voice Portal Software Tomcat Web Application Vulnerability<br>Calculate the environmental score of | | | | | |
|---|---|---|---|---|---|
| CVSS Base Score - **10.0** | | | | | |
| Access Vector | Access Complexity | Authentication | Confidentiality Impact | Integrity Impact | Availability Impact |
| Network | Low | None | Complete | Complete | Complete |
| CVSS Temporal Score - **8.3** | | | | | |
| Exploitability | | Remediation Level | | Report Confidence | |
| Functional | | Official-Fix | | Confirmed | |

| CSCub38379 - Cisco Unified Customer Voice Portal Software Tomcat Configuration 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 | Complete | None |
| CVSS Temporal Score - **6.4** | | | | | |
| Exploitability | | Remediation Level | | Report Confidence | |
| Functional | | Official-Fix | | Confirmed | |

| CSCub38372 - Cisco Unified Customer Voice Portal Software File Access 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 | Complete | None | None |

| CVSS Temporal Score - **6.4** | | |
|---|---|---|
| Exploitability | Remediation Level | Report Confidence |
| Functional | Official-Fix | Confirmed |

| **CSCub38369 - Cisco Unified Customer Voice Portal Software Path Traversal Vulnerability Calculate the environmental score of** | | | | | |
|---|---|---|---|---|---|
| CVSS Base Score - **7.1** | | | | | |
| Access Vector | Access Complexity | Authentication | Confidentiality Impact | Integrity Impact | Availability Impact |
| Network | Medium | None | None | Complete | None |
| CVSS Temporal Score - **5.9** | | | | | |
| Exploitability | | Remediation Level | | Report Confidence | |
| Functional | | Official-Fix | | Confirmed | |

| **CSCub38366 - Cisco Unified Customer Voice Portal Software XML Entity Expansion Vulnerability Calculate the environmental score of** | | | | | |
|---|---|---|---|---|---|
| CVSS Base Score - **7.8** | | | | | |
| Access Vector | Access Complexity | Authentication | Confidentiality Impact | Integrity Impact | Availability Impact |
| Network | Low | None | Complete | None | None |
| CVSS Temporal Score - **6.4** | | | | | |
| Exploitability | | Remediation Level | | Report Confidence | |
| Functional | | Official-Fix | | Confirmed | |

## 影響

これらの脆弱性が不正利用されると、さまざまな影響が生じる可能性があります。

Cisco Bug ID CSCua65148（ 登録ユーザ専用 ）として文書化されている Cisco Unified Customer Voice Portal ソフトウェアの SIP INVITE パケットの脆弱性が不正利用されると、認証されていないリモートの攻撃者がシステムの新規コール受付不能を引き起こす可能性があります。

Cisco Bug ID CSCub38384（ 登録ユーザ専用 ）として文書化されている Cisco Unified Customer Voice Portal ソフトウェアの Tomcat Web アプリケーションの脆弱性が不正利用されると、認証されていないリモートの攻撃者が権限を昇格し、管理者アクセス権を取得する可能性があります。

Cisco Bug ID CSCub38379（ 登録ユーザ専用 ）として文書化されている Cisco Unified Customer Voice Portal ソフトウェアの Tomcat 構成の脆弱性が不正利用されると、認証されていないリモートの攻撃者が、許可されていないユーザから提供された Web アプリケーションを実行する可能性があります。

Cisco Bug ID CSCub38372（ 登録ユーザ専用 ）として文書化されている Cisco Unified Customer Voice Portal ソフトウェアの XML エンティティ拡張の脆弱性が不正利用されると、認証されていないリモートの攻撃者が任意のシステム ファイルを閲覧する可能性があります。

Cisco Bug ID CSCub38369（ 登録ユーザ専用 ）として文書化されている Cisco Unified Customer Voice Portal ソフトウェアのパス トラバーサルの脆弱性が不正利用されると、認証されていないリモートの攻撃者がシステム ファイルを上書きする可能性があります。

Cisco Bug ID CSCub38366（ 登録ユーザ専用 ）として文書化されている Cisco Unified Customer Voice Portal ソフトウェアの XML エンティティ拡張の脆弱性が不正利用されると、認証されていないリモートの攻撃者が任意のシステム ファイルを閲覧す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

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。

これらの脆弱性は、Cisco Unified CVP ソフトウェア バージョン 9.0.1 ES 11 で修正されています。お客様には、このバージョン以降へのアップグレードを推奨いたします。

Cisco Unified CVP ソフトウェア バージョン 9.0.1 ES 11は次のリンクでダウンロード可能です。

http://software.cisco.com/download/special/release.html?config=c51444496bd899c41331b5ad20b97954

他のCisco Unified CVP ソフトウェアのダウンロードについては次のリンクをご参照ください。

http://software.cisco.com/download/type.html?mdfid=270563413&catid=null/

バージョン 8.x ソフトウェアは2013年7月に利用可能になる予定です。ソフトウェアが利用可能になりましたら、この文書にてリンク情報をアップデートいたします。

## 回避策

Cisco Unified Customer Voice Portal ソフトウェアの XML エンティティ拡張の脆弱性に対する回

避策は Cisco Bug ID CSCub38366（登録ユーザ専用）として文書化されています。

Cisco Unified Customer Voice Portal ソフトウェアの XML エンティティ拡張の脆弱性に対する回避策を実施するには、Cisco Unified CVP デバイス間の通信が SSL で保護されている必要があります。Cisco Unified CVP デバイス間の通信を保護する方法については、 次のリンクにある『*Configuration and Administration Guide for Cisco Unified CVP*』の「Unified CVP security」セクションを参照してください。

http://www.cisco.com/en/US/docs/voice_ip_comm/cust_contact/contact_center/customer_voice_portal/cvp9_0/configuration/guide/CCVP_BK_CA6D87A1_00_cvp-configuration-and-administration-guide.pdf

Cisco Unified Customer Voice Portal ソフトウェアのTomcat Web アプリケーションの脆弱性に対する回避策は Cisco Bug ID CSCub38379（ 登録ユーザ専用）として文書化されています。

Cisco Unified Cutomer Voice Portal ソフトウェアの Tomcat Web アプリケーションの脆弱性に対する回避策を実施するためには、CVP サーバのTomcat インスタンスから手動でManager および Host-Manager web アプリケーションを削除する必要があります。

CVP VXML server
C:¥Cisco¥CVP¥VXMLServer¥Tomcat¥server¥webapps に移動し、Manger および Host-Manager フォルダーを削除します。

CVP Call Server
C:¥Cisco¥CVP¥VXMLServer¥Tomcat¥server¥webapps に移動し、Manger および Host-Manager フォルダーを削除します。

CVP Operation Console Server
C:¥Cisco¥CVP¥VXMLServer¥Tomcat¥server¥webapps に移動し、Manger および Host-Manager フォルダーを削除します。

CVP Reporting Server
C:¥Cisco¥CVP¥VXMLServer¥Tomcat¥server¥webapps に移動し、Manger および Host-Manager フォルダーを削除します。

このドキュメントで公開されている他の脆弱性に対する回避策はありません。

回避策の詳細は、このアドバイザリの付属ドキュメントである『Applied Mitigation Bulletin（AMB）』にて参照できます。

http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=28982/

## 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。

この脆弱性は Alex Senkevitch 氏からシスコにご報告いただきました。

# 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-20130508-cvp/

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 1.1 | 2013-May-10 | Updated Workaround and Software Versions sections. |
| Revision 1.0 | 2013-May-08 | 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。