Cisco Unified Contact Center Express の脆弱性

High

アドバイザリーID : cisco-sa-20100609-uccx

初公開日 : 2010-06-09 16:00

バージョン 1.0 : Final

CVSSスコア : 7.8

回避策 : No Workarounds available

Cisco バグ ID :

CVE-2010-1571

CVE-2010-1569

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 Unified Contact Center Express （ UCCX か統一された CCX ）はサービス拒否 （ DoS ）脆弱性およびディレクトリ トラバーサルの脆弱性が含まれています。 これらの脆弱性は相互に関連していません。

これらの脆弱性の不正利用は DoS 状態か情報の漏えいという結果に終る可能性があります。

Cisco は Cisco Unified Contact Center 製品の最新バージョンの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ました。

このアドバイザリは 609-uccx で掲示されます。

該当製品

Cisco UCCX は 300 までのエージェントの配備の使用のための統合された「ボックスのコンタクトセンター」ソリューションです。

脆弱性のある製品

この文書に説明がある脆弱性は以下の製品に影響を及ぼします:

- Cisco UCCX バージョン 5.x、6.x および 7.x
- Ciscoカスタマー 応答ソリューション （ CRS ）バージョン 5.x、6.x および 7.x
- Cisco Unified IP Interactive Voice Response （ IVR ） （ Cisco Unified IP IVR ）バージョン 5.x、6.x および 7.x

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 UCCX 製品のコンピュータ テレフォニー インテグレーション（CTI）サーバコンポーネントで存在 する DoS 脆弱性。 CTI サーバは CTI サーバ DoS 脆弱性から Integrated Call Distribution（ICD）ライセンスが有効に なるとき開始された、Cisco Unified IP Interactive Voice Response（IVR）（Cisco Unified IP IVR）配備だけ影響を受けませんです。 CTI サーバは TCPポート 42027 でポート番号がシステム ポートパラメータ 画面で変更することができるが、デフォルトで受信します。 この脆弱性は CTI サーバおよび Cisco Unified CCX Node Manager が失敗します可能性があるすべての活動中のエージェントはログアウトされます脆弱 なシステムに当たる 不正 な CTI メッセージによって引き起こされ。 DoS 状態は一時的であり、Cisco UCCX システムは再度操作上に一度 Node Manager なり、CTI サーバは自動再始動を完了します。

この脆弱性は Cisco バグ ID CSCso89629（登録ユーザのみ）で文書化されています、CVE ID CVE-2010-1570 を割り当てられました。

ディレクトリ トラバーサルの脆弱性

システムのあらゆるファイルに読み取り アクセスを許可する Cisco UCCX 製品のブートストラップ サービスで存在 する ディレクトリ トラバーサルの脆弱性。 この脆弱性は TCPポート 6295 に当たるブートストラップ メッセージによって引き起こされます。 ブートストラップ サービスがハイアベイラビリティ配置 モ デルで UCCX 設定をサーバを渡って同期しておくのに利用されています。 すべての配置モードは第 2 ノードが設定に追加されたときだけ、ICD のような、影響を受けます ICM および IP-IVR。（ノードは**システム** プルダウン タスクバーの**サーバオプション**の Cisco UCCX 管理 Webインターフェイスを使用してリストされます）。 システムが脆弱であることができるようにハイアベイラビリティ ライセンスが必要となりません。

この脆弱性は Cisco バグ ID CSCsx76165（登録ユーザのみ）で文書化されています、CVE ID CVE-2010-1571 を割り当てられました。

セキュリティ侵害の痕跡

回避策

これらの脆弱性に対する回避策はありません。

ネットワークの on Cisco 配置されたデバイスの場合もある追加軽減は次のリンクで利用可能のこのアドバイザリに Cisco によって加えられる軽減情報ドキュメントガイドで利用できます、: 609-uccx。

修正済みソフトウェア

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 およびそれ以降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機器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。 情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

次 の テーブルはこの文書に説明がある脆弱性から影響を受ける Cisco UCCX のバージョンを表します。 すべての脆弱性は製品の最新バージョンで解決されます。

CSCso89629 CTI サービス DoS 脆弱性（Cisco UCCX）

リリース値でフィルタリングする	脆弱	固定される第 1
8.0	脆弱性なし	
7.0	脆弱	7.0(1)SR4、7.0(2)
6.0	脆弱	6.0(1)SR1
5.0	脆弱	5.0(2)SR3

CSCsx76165 ブートストラップ サービス 案内公開脆弱性（Cisco UCCX）

リリース値でフィルタリングする	脆弱	固定される第 1
8.0	脆弱性なし	
7.0	脆弱	7.0(1)SR2、7.0(2)
6.0	脆弱	修正済みリリースへのアップデート
5.0	脆弱	5.0(2)SR3

不正利用事例と公式発表

このアドバイザリで説明されている脆弱性の公表や悪用に関する情報は Cisco PSIRT には寄せられていません。

DoS 脆弱性は Cisco 内部テストの間に発見され、ブートストラップ サービス ディレクトリ トラバーサルの脆弱性は顧客によって Cisco Technical Assistance Center （TAC）に報告されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100609-uccx

改訂履歴

リビジョン 1.0	2010-June-09	初回公開リリース

利用規約