Cisco CallManager/Unified Communications Manager のログオン ページにおける XSS と SQL インジェクション

アドバイザリーID : cisco-sa-20070829-ccm CVE-2007-4633
初公開日 : 2007-08-29 16:00
バージョン 1.2 : Final
CVSSスコア : 5.0
回避策 : No Workarounds available
Cisco バグ ID :

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 CallManager および Unified Communications Manager は、管理者またはユーザのログオン ページの lang 変数におけるクロスサイト スクリプティング（XSS）および SQL インジェクション攻撃に対する脆弱性を含んでいます。攻撃に成功した場合、攻撃者は CallManager または Unified Communications Manager に接続されているコンピュータ システム上で JavaScript を実行したり、データベース内の情報を参照したりすることができます。

Cisco では、該当するお客様用に、これらの脆弱性に対応する無償ソフトウェアを提供しております。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070829-ccm で公開されています。

該当製品

脆弱性のある製品

次のバージョンよりも前の Cisco CallManager および Unified Communications Manager は、これらの脆弱性に該当します。

- 3.3(5)sr2b
- 4.1(3)sr5
- 4.2(3)sr2
- 4.3(1)sr1

CallManager または Unified Communications Manager システムのソフトウェア バージョンを調べるには、管理インターフェイスで Show > Software の順に選択します。

Unified Communications Manager バージョン 5.0 の場合は、コマンド ライン インターフェイス（CLI）で show version active を実行してソフトウェア バージョンを調べることもできます。

CallManager または Unified Communications Manager バージョン 3.x および 4.x システムの場合は、管理インターフェイスで Help > About Cisco Unified CallManager の順に選択し、Details ボタンをクリックしてソフトウェア バージョンを調べることができます。

注：Cisco Unified CallManagerバージョン4.3、5.1、および6.0の名称は、Cisco Unified Communications Managerに変更されています。ソフトウェア バージョン 3.3、4.0、4.1、4.2、および 5.0 は、Cisco Unified CallManager の名称を保持しています。

脆弱性を含んでいないことが確認された製品

この脆弱性に該当するその他の Cisco 製品は現在のところ見つかっていません。

他のバージョンの CallManager および Unified Communications Manager は、これらの脆弱性には該当しません。

詳細

Cisco Unified CallManager/Communications Manager（CUCM）は、企業のテレフォニー機能を IP Phone、メディア処理デバイス、Voice-over-IP（VoIP）ゲートウェイ、マルチメディア アプリケーションなどのパケット テレフォニー ネットワーク デバイスに拡張する Cisco IP テレフォニー ソリューションのコール処理コンポーネントです。

クロスサイト スクリプティングの脆弱性と SQL インジェクションの脆弱性は、特別に細工された値が管理者またはユーザのログオン ページの lang 変数で入力された場合に発生します。これらの脆弱性に対する攻撃は、Web インターフェイスを介して実行され、http または https プロトコルが使用されます。クロスサイト スクリプティングの脆弱性では、<script> タグと </script> タグに囲まれたスクリプティング コードが悪意のある値に含まれます。SQL インジェクションの脆弱性では、この値によって SQL 呼び出しが終了され、バックエンド データベースへの呼び出しが実行されます。

攻撃者がクロスサイト スクリプティングの脆弱性を悪用するには、特別に細工された URL をユーザに入力させる必要があります。

クロスサイトスクリプティングの脆弱性は、Bug ID CSCsi10728 (登録ユーザ専用)に記載されています。

SQLインジェクションの脆弱性は、Bug ID CSCsi64265 (登録ユーザ専用)に記載されています。

回避策

これらの脆弱性に対する回避策はありません。

クロスサイト スクリプティング（XSS）は、悪意のあるユーザ、脆弱な Web サイト、悪意のある Web サイトの所有者が、疑いを持っていないユーザに悪意のあるコードを送信するために悪用できる Web アプリケーションの欠陥です。通常、悪意のあるコードはリンクの URL に埋め込まれたスクリプトの形で存在し、このコードが脆弱なサーバまたは悪意のある Web サイトに格納されます。このような Web コンテンツは信頼できるサイトのものであると想定され、ブラウザには URL または HTML コンテンツを検証する方法がないため、ブラウザで悪意のあるコードが実行されます。XSS 攻撃の主な送信元は、動的に生成される Web ページにユーザが送信したコンテンツを適切に検証しない Web サイトです。

XSS の脆弱性の性質上、ネットワークにおける緩和テクニックは一般的に効果がありません。ユーザが XSS 攻撃の犠牲者になるリスクを減らすには、ブラウザの URL 検証の制限に関する情報をユーザに提供する必要があります。また、スクリプティング制御を通じてブラウザ内で対応策を実装することもできます。スクリプティング制御を使用すると、コードの実行を制限するポリシーを定義できます。

XSS 攻撃とこれらの脆弱性を悪用するために使用される方法についての詳細は、http://www.cisco.com/warp/public/707/cisco-air-20060922-understanding-xss.shtml にある Cisco 適用インテリジェンス レスポンス『クロスサイト スクリプティング（XSS）脅威ベクトルについて』を参照してください。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況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。

いかなる場合も、アップグレードを予定しているデバイスに十分なメモリがあり、現在のハードウェアおよびソフトウェア構成が新しいリリースで適切にサポートされ続けることを必ず確認してください。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。

バージョン	修正済みリリース	ダウンロード場所
3.3	3.3(5)sr2b	http://www.cisco.com/pcgi-bin/tablebuild.pl/callmgr-33?psrtdcat20e2（登録ユーザのみ）

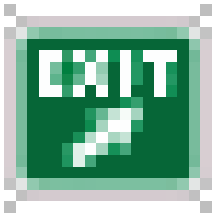
4.1	4.1(3)sr5	http://www.cisco.com/pcgi-bin/tablebuild.pl/callmgr-41?psrtdcat20e2 (登録ユーザのみ)
4.2	4.2(3)sr2	http://www.cisco.com/pcgi-bin/tablebuild.pl/callmgr-42?psrtdcat20e2 (登録ユーザのみ)
4.3	4.3(1)sr1	http://www.cisco.com/pcgi-bin/tablebuild.pl/callmgr-43?psrtdcat20e2 (登録ユーザのみ)

推奨事項

$propertyAndFields.get("recommendations")

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悪用に関する情報は Cisco PSIRT に寄せられていませんが、公表内ですでに議論されています。次のような参考資料があります。

http://packetstormsecurity.org/0708-exploits/cisco-sql.txt にアクセスしてください。 

この脆弱性は Gama SEC および Brandeis 大学の Elliot Kendall 氏により Cisco に報告されたものです。Cisco では、この問題を報告し、この問題の発表にご協力いただいた Gama SEC ならびに Elliot Kendall 氏に対して謝意を表します。Cisco では、研究者と協力してセキュリティ脆弱性に関する調査を進め、製品レポートで発表することを常に歓迎しています。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070829-ccm

改訂履歴

リビジ	2008年4月	CSCsi10728およびCSCsi64265の

ョン 1.2	25日	CVSSスコアへのリンクを更新。
リビジョン 1.1	2007 年 8 月 31 日	「不正利用と公表」セクションで、表現を変更し、リンクを追加。
リビジョン 1.0	2007 年 8 月 29 日	初版リリース

利用規約

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も示唆するものではありません。 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、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。