Cisco Unified Communications Managerの複数のDoS脆弱性

アドバイザリーID : cisco-sa-20130227-cucm
初公開日 : 2013-02-27 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 : CSCtx43337 CSCub28920

CVE-2013-1134
CVE-2013-1133

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 Communications Managerには2つの脆弱性があり、認証されていないリモートの攻撃者がサービス妨害(DoS)状態を引き起こす可能性があります。これらの脆弱性が不正利用されると、音声サービスの中断が引き起こされる可能性があります。

シスコは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ています。このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130227-cucm

該当製品

脆弱性のある製品

次の製品は、このアドバイザリに記載された脆弱性の影響を受けます。

- Cisco Unified Communications Manager 8.6(x)
- Cisco Unified Communications Manager 9.0(x)

注：Cisco Unified Communications Managerバージョン6.1は、2011年9月3日にソフトウェアメンテナンスが終了しています。Cisco Unified Communications Manager 6.xバージョンをご使用のお客様は、サポートされているCisco Unified Communications Managerのバージョンへのアップグレードに関してシスコサポートチームにお問い合わせください。

脆弱性を含んでいないことが確認された製品

次の製品は、このアドバイザリに記載された脆弱性の影響を受けません。

- Cisco Unified Communications Manager 7.x
- Cisco Unified Communications Manager 8.5(x)

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 Communications Managerは、Cisco IP Telephonyソリューションのコール処理コンポーネントであり、企業のテレフォニー機能を、IP電話、メディア処理デバイス、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します。

不正なUDPパケットに起因するDoS脆弱性

Cisco Unified Communications ManagerにはDoS脆弱性があり、認証されていないリモートの攻撃者がCPUのリソースを枯渇させる可能性があります。この脆弱性は、未使用のUDPポートで不正なパケットを受信することによって引き起こされ、Graphical User Interface（GUI；グラフィカルユーザインターフェイス）に接続できず、音声サービスが中断する可能性があります。

この脆弱性は、Cisco Bug ID CSCtx43337(登録ユーザ専用)として文書化され、Common Vulnerabilities Enumerator(CVE)IDとしてCVE-2013-1133が割り当てられています。この脆弱性は、Cisco Unified Communications Managerバージョン8.6(x)以降に適用され、Cisco Unified Communications Managerバージョン9.0(1)、8.6(4) BE3k、および8.6(2a)su2で修正されています。Cisco Unified Communications Manager 7.1(x)および8.5(x)バージョンは影響を受けません。

Location Bandwidth Manager(LBM)キャッシュ汚染の脆弱性

Cisco Unified Communications Manager 9.0には、認証されていないリモートの攻撃者がLocation Bandwidth Manager(LBM)のトランザクションレコードを汚染する可能性のある脆弱性が存在します。

この脆弱性は、LBM間のクラスタ内通信におけるリモートLBMハブノードの認証の欠如に起因します。攻撃者は、LBMトランザクションレコードをポイズニングしてすべての使用可能な帯域幅プールを消費させることで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はすべての帯域幅を消費し、コールを拒否する可能性があります。この脆弱性は、Cisco Bug ID CSCub28920(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-1134が割り当てられています。この脆弱性は、Cisco Unified Communications Managerバージョン9.0(x)にのみ適用され、Cisco Unified Communications Managerバージョン9.1(1)で修正されています。

Cisco Unified Communications Manager 7.1(x)、8.5(x)、および8.6(x)バージョンは影響を受けません。

回避策

信頼できない送信元からのトラフィックをTCPポート9004でフィルタリングすると、LBMの脆弱性を回避できます。

ネットワーク内のシスコデバイスに適用可能な他の対応策は、次のリンクにある付属ドキュメント『Identifying and Mitigating Exploitation of the Cisco Unified Communications Manager and Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability』に記載されています。 https://sec.cloudapps.cisco.com/security/center/viewAMBAlert.x?alertId=28034

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。シスコでは、表の「Recommended Release」列のリリース、またはそれ以降のリリースにアップグレードすることを推奨しています。

Cisco Unified Communication Managerバージョン	推奨リリース
8.x	8.6(4)BE3K、8.6(2a)su2
9.x	9.1(1)

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。

推奨事項

$propertyAndFields.get("recommendations")

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エクスプロイト事例とその公表は確認しておりません。

これらの脆弱性は内部テストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130227-cucm

改訂履歴

リビジョン 1.0	2013年2月27日	初回公開リリース

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。