

Cisco Tivoli Business Service ManagerのDoS脆弱性

Medium	アドバイザーID : Cisco-SA-20130406-CVE-2013-1174	CVE-2013-1174
	初公開日 : 2013-04-06 19:38	
	バージョン 1.0 : Final	
	CVSSスコア : 5.0	
	回避策 : No Workarounds available	
	Cisco バグ ID : CSCue03703	

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 Hosted Collaboration Mediation(HCM)の一部であるCisco Tivoli Business Service Manager(TBSM)には、認証されていないリモートの攻撃者が部分的なサービス妨害(DoS)を引き起こす可能性のある脆弱性が存在します。

攻撃者は、Cisco TBSM上のポート17310 ~ 17542に向けて大量のTCPパケットを送信することにより、この脆弱性を不正利用する可能性があります。攻撃に成功すると、攻撃が続いている間に特定のサービスが停止する可能性があります。

シスコはセキュリティ通知で脆弱性を確認しましたが、ソフトウェアアップデートは利用できません。

この脆弱性をエクスプロイトするには、攻撃者は信頼できる内部ネットワークにアクセスして、一連のTCPパケットをターゲットシステムに送信する必要があります。このアクセス要件により、攻撃が成功する可能性が低くなる可能性があります。

影響を受けるバージョンの最新のリストについては、ベンダー発表セクションのバグレポートを参照してください。

該当製品

シスコは、[CVE-2013-1174](#)のリンクで、バグID [CSCue03703](#)のセキュリティ通知をリリースしました。

脆弱性のある製品

このアラートが最初に公開された時点では、Cisco TBSMバージョン9.0には脆弱性が存在していました。Cisco TBSMの新しいバージョンも影響を受ける可能性があります。

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。

回避策

今後のアップデートやリリースについては、ベンダーに連絡することを推奨します。

信頼できるユーザだけにネットワークアクセスを許可することを推奨します。

影響を受けるシステムを監視することを推奨します。

修正済みソフトウェア

ソフトウェアの更新プログラムは利用できません。

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) 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やその公表を確認していません。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20130406-CVE-2013-1174>

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初版リリース	適用外	Final	2013年4月6日

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、単独の転載や意識を施した場合、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。