

Cisco Building Broadband Service Managerのクロスサイトスクリプティングの脆弱性



アドバイザリーID : Cisco-SA-20080514- [CVE-2008-2165](#)
CVE-2008-2165
初公開日 : 2008-05-14 17:52
バージョン 1.0 : Final
CVSSスコア : [4.3](#)
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 Building Broadband Service Manager(BBSM)5.3 SP2以前には、認証されていないリモートの攻撃者によるクロスサイトスクリプティング(XSS)攻撃を可能にする脆弱性が存在します。

この脆弱性は、BBSM Webインターフェイスに関連付けられた特定のWebページでの入力検証エラーが原因で存在します。 攻撃者は、クロスサイトスクリプティング攻撃を実行するために設計された巧妙に細工されたリンクに認証されたユーザを誘導することで、この脆弱性を不正利用する可能性があります。 不正利用に成功すると、攻撃者はターゲットユーザの特権を使用してシステム上で任意のスクリプトコードを実行する可能性があります。

この脆弱性の実証には、概念実証URLを使用できます。

シスコはこの脆弱性をCisco Bug IDで確認し、修正するためのパッチをリリースしました。

攻撃者は電子メールまたは他の形式のメッセージングで送信される悪意のあるリンクに従うようにユーザを誘導する必要があるため、この脆弱性を不正利用するにはソーシャルエンジニアリング手法を採用する必要があります。 攻撃者はこの脆弱性を直接悪用できず、ユーザの操作に依存して攻撃の可能性を低減する必要があります。

攻撃者は、ユーザのCookieや最近送信されたデータにアクセスできる可能性があります。 攻撃者は、該当するソフトウェアのターゲットユーザとしてアクションを実行できる可能性もあります。

該当製品

シスコは次のリンクで登録ユーザ向けにCisco Bug IDをリリースしています。 [CSCso62583](#)

脆弱性のある製品

Cisco BBSMバージョン5.3 SP2以前には脆弱性が存在します。

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

この脆弱性に対処するには、BBSMパッチ5322を適用することをお勧めします。

信頼できない送信元からの電子メールメッセージを開かないようにすることを推奨します。

未承諾のリンクは使用しないことをお勧めします。 ユーザは、予期しないリンクを追跡する前に、その信頼性を確認する必要があります。

クロスサイトスクリプティング攻撃と方法の詳細については、シスコの適用対応策のドキュメント『[クロスサイトスクリプティングの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

契約が有効なシスコのお客様は、[Cisco](#)のSoftware Centerからアップデートを入手できます。契約をご利用でないお客様は、Cisco Technical Assistance Center(TAC)に1-800-553-2447または1-408-526-7209で連絡するか、tac@cisco.comに電子メールで問い合わせせてアップグレードを入手できます。

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) 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-20080514-CVE-2008-2165>

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	2008年5月14日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。