

# Ciscoオンラインヘルプシステム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-20070315-[CVE-2007-1467](#)  
CVE-2007-1467  
初公開日 : 2007-03-15 20:15  
バージョン 1.0 : Final  
CVSSスコア : [1.9](#)  
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

複数のシスコ製品に、オンラインヘルプシステムに存在する脆弱性により、認証されていないリモートの攻撃者がクロスサイトスクリプティング攻撃を実行する可能性があります。

この脆弱性は、WebベースのOnline Help Systemインターフェイスの検索機能が、ユーザが指定した入力を十分にフィルタリングできないために存在します。認証されていないリモートの攻撃者が、巧妙に細工されたリンクにユーザを誘導してこの脆弱性を不正利用する可能性があります。

シスコは、セキュリティ応答でこの脆弱性を確認し、承認済みの回避策を発行しました。

攻撃者は、この脆弱性を直接悪用することはできません。代わりに、巧妙に細工されたリンクに従うようにユーザを説得する必要があります。攻撃者が該当サイトのコンテキストで任意のスクリプトコードを実行し、機密のブラウザ情報にアクセスしたり、ユーザとして該当サイトでアクションを実行したりできる可能性があります。

影響を受ける製品の多くは貴重な資産と考えられるため、この脆弱性は企業のスパイ活動に投資されている攻撃者の注目を集める可能性があります。競合他社のデータストリーム、ネットワーク、またはVoIP電話システムにアクセスする機能は、盗まれた情報を扱う個人にとって選択の結果です。

影響を受けるシステム上でメンテナンスタスクを実行する際には、迷惑リンクを使用しないことを強く推奨します。また、管理者は、管理セッションの完了後にログアウトして、有効な認証ク

ッキーが管理者ワークステーションに残らないようにしなければなりません。

## 該当製品

シスコは、Cisco Bug ID CSCsh91761(Secure ACS)、CSCsh52300(VPN Client)、CSCsh91884(Unified Personal Communicator)、CSCsi12435(MeetingPlace)、CSCsh91901(MeetingPlace Express)、CSCsh99191999999990001に0対応1の0セキュリティ1を20000000000 CSCsh91953(IP Communicator)、CSCsh93070(Unified Video Advantage)、CSCsh93854 ( ビデオ会議 )、CSCek71039(WAN Manager)、CSCsh95009(Security Device Manager)、CSCsi10818(NAM)、CSCsi10674(CSCSCk93854) CiscoWorks)およびCSCsi10982(Wireless LAN Solution Engine)を参照してください。リンクはcisco-sr-20070315-xssです。

### 脆弱性のある製品

Online Help Systemコンポーネントを含むシスコ製品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

アップデートは利用可能になった時点で適用することをお勧めします。

信頼できないWebサイトにはアクセスしないことをお勧めします。

信頼できないソースからのリンクに従わないようお勧めします。 リンクを辿る前に、リンクの真正性を確認することをお勧めします。

管理者は、PreSearch.htmlファイルとPreSearch.classファイルの削除または名前の変更を検討できます。

管理者は、セッションを完了した後に管理インターフェイスからログアウトすることを推奨します。

## 修正済みソフトウェア

パッチまたはソフトウェアアップデートは利用できません。

## 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-20070315-CVE-2007-1467>

## 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	2007年3月15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。