CiscoWorks Common Services フレームワーク ヘルプ Servlet クロスサイト スクリプティング脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20110518-CVE-2011-0961 **初公開日 :** 2011-05-18 13:17 **最終更新日 :** 2012-07-14 13:00 **バージョン 2.0 :** Final **CVSSスコア :** 4.3 **回避策 :** No Workarounds available **Cisco バグ ID :**	CVE-2011-0961

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

CiscoWorks Common Services は非認証を可能にする可能性があるクロスサイト スクリプティング攻撃を行なうためにクロスサイト スクリプティング脆弱性がリモート攻撃者含まれています。

脆弱性は影響を受けたアプリケーションに URL パラメータによって供給される形式が間違ったユーザインプットの不適当な検証が原因です。 非認証はユーザの悪意のあるリンクを表示するように確信によって、リモート攻撃者この脆弱性を不正利用する可能性があります。 成功すれば、攻撃者は影響を受けたサイトのセキュリティ コンテキストのユーザーのブラウザーの任意スクリプトか HTML コードを実行する可能性があります。

エクスプロイト コードは利用できます。

Cisco はこの脆弱性を確認し、更新済ソフトウェアをリリースしました。

この脆弱性を不正利用するために、攻撃者はユーザを悪意のあるリンクに従うように確信させる必要があります。 攻撃者は E メールまたは即刻メッセージのリンクを提供するかもしれません。

ユーザーのブラウザーの悪意のあるスクリプトを実行する機能を示す機能エクスプロイト コードは共用利用可能です。

この脆弱性は安心感の Brett Gervasoni によって Cisco 社に検出され、報告されました。

該当製品

Cisco は Cisco バグ ID CSCto12704 （登録ユーザ）の脆弱性を確認しました。

脆弱性のある製品

CiscoWorks Common Services バージョン 3.3 は前に脆弱であり。

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

管理者は適切な更新を加えるように助言されます。

ユーザは疑わしくか認識されないソースからの電子メール メッセージを開かないように助言されます。 電子メール メッセージに含まれているリンクか添付ファイルは安全であることをユーザが確認できなければ、それらを開かないように助言されます。

管理者は影響を受けたシステムを監視するように助言されます。

修正済みソフトウェア

アクティブな契約を持つ Cisco カスタマは次のリンクで Software Center を通して更新を入手できます: Cisco。 契約のない Cisco カスタマは 1-800-553-2447 か 1-408-526-7209 でまたは tac@cisco.com で E メールで Cisco Technical Assistance Center にコンタクトをとってアップグレードを入手できます。

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やその公表を確認していません。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20110518-CVE-2011-0961

改訂履歴

Version	Description	Section	Status	日付
1.0	初版リリース	該当なし	Final	2011-May-18

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。