

# CiscoWorks TFTP ディレクトリ トラバーサルの脆弱性

**Critical** アドバイザリーID : cisco-sa-[CVE-20090520-cw](#)  
初公開日 : 2009-05-20 16:00 [2009-1161](#)  
バージョン 1.0 : Final  
CVSSスコア : [10.0](#)  
回避策 : [Yes](#)  
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

CiscoWorks Common Services はアクセス アプリケーションに非認証リモート攻撃者を可能にし、オペレーティング システム ファイルをホストする可能性がある脆弱性が含まれています。

シスコはこ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ました。この脆弱性に対しては回避策があります。

このアドバイザリーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090520-cw> で掲示されます。

## 該当製品

### 修正済みソフトウェア

有効になる TFTP サービスがある CiscoWorks Common Services バージョン 3.0.x を実行し、製品、3.1.x および 3.2.x に脆弱です。Microsoft Windows オペレーティング システムで稼動する CiscoWorks Common Services システムだけ影響を受けています。

ベースがこの脆弱性から影響を受けると同時に CiscoWorks Common Services を使用する以下のシスコ製品。

- Cisco Unified サービス モニタバージョン 1.0、1.1、2.0、および 2.1
- CiscoWorks QoS Policy Manager バージョン 4.0 および 4.1
- CiscoWorks LAN Management Solution バージョン 2.5、2.6、3.0、3.0.1 および 3.1

- Cisco Security Manager バージョン 3.0、3.1、および 3.2
- Cisco TelePresence Readiness Assessment Manager バージョン 1.0
- CiscoWorks Voice Manager バージョン 3.0 および 3.1
- CiscoWorks Health and Utilization Monitor バージョン 1.0 および 1.1
- Cisco Unified オペレーション マネージャバージョン 1.0、1.1、2.0、および 2.1

CiscoWorks Common Services の Solarisバージョンはこの脆弱性から影響を受けません。

TFTPサービスはデフォルトで有効になります。TFTPサービスが CiscoWorks インターフェイスに接続する動作している **Services** ウィンドウにアクセスするために Start > Settings > Control Panel > Administrative Tools > Services の順に選択 すればことを確認するために。サービスの名前は **CWCS TFTPサービス**です。

注: 管理者はまた命じますシステムで動作しているサービスをリストするために **tasklist/SVC** Microsoft ウィンドウを発行できます。

## 脆弱性を含んでいないことが確認された製品

CiscoWorks Common Services バージョン 3.0.x、3.1.x および 3.2.x を使用しないかまたは有効になる TFTP サービスがない製品は脆弱ではないです。CiscoWorks Common Services の Solarisバージョンはこの脆弱性から影響を受けません。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。

### 改訂履歴

リビジョン 1.0	2009-May-20	初版リリース
-----------	-------------	--------

### 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。