Wireless Control System の複数の脆弱性

severity	**アドバイザリーID :** cisco-sa-20060628-wcs **初公開日 :** 2006-06-28 16:00 **バージョン 1.2 :** Final **回避策 :** Yes **Cisco バグ ID :**	CVE-2006-3289 CVE-2006-3287 CVE-2006-3288 CVE-2006-3285 CVE-2006-3290

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 Wireless Control System（WCS）には、リモート ユーザによる次の操作を可能にする複数の脆弱性があります。

- WCS によって管理されているアクセス ポイントに関する機密の設定情報にアクセスする
- WCS システム上の任意のファイルを読み書きする
- デフォルトの管理者パスワードを使用して WCS システムにログインする
- WCS ユーザの Web ブラウザでスクリプト コードを実行する
- 機密の WCS 設定情報が保存されているディレクトリにアクセスする

これらの脆弱性の一部に関しては回避策があります。 詳細については、「回避策」のセクションを参照してください。 Cisco では、該当するお客様用に、これらの脆弱性に対応する無償ソフトウェアを提供しております。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060628-wcs で掲示されます。

該当製品

修正済みソフトウェア

DDTS	該当するリリース
CSCsd15955	WCS for Linux and Windows 3.2(40) 以前
CSCsd15951	WCS for Linux and Windows 3.2(51) 以前
CSCse21391	WCS for Linux and Windows 4.0(1) 以前
CSCsd71397	WCS for Linux and Windows 3.2(51) 以前
CSCse01127	WCS for Linux and Windows 3.2(51) 以前
CSCse01409	WCS for Linux and Windows 3.2(51) 以前

特定のデバイスにインストールされている WCS ソフトウェアのバージョンは、WCS HTTP 管理インターフェイスで調べることができます。 ソフトウェアのバージョンを調べるには、**Help -> About the Software** の順に選択します。

特定のデバイスにインストールされている WCS ソフトウェアのバージョンは、WCS HTTP 管理インターフェイスで調べることができます。 ソフトウェアのバージョンを調べるには、**Help -> About the Software** の順に選択します。

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。

改訂履歴

リビジョン 1.2	2007 年 6 月 1 日	DDTS CSCse21391 のソフトウェア バージョンと修正の表をわずかに変更
リビジョン 1.1	2006 年 6 月 28 日	説明をわずかに変更
リビジョン 1.0	2006 年 6 月 28 日	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。