Cisco Collaboration サーバ脆弱性

severity	**アドバイザリーID :** cisco-sa-20040630-CCS	CVE-2004-0650
	初公開日 : 2004-06-30 16:00	
	バージョン 1.0 : Final	
	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

Cisco Collaboration サーバ（CCS）バージョンは ServletExec バージョンと先に許可されていないユーザがファイルをアップロードし、管理権限を得ることができる攻撃に脆弱であるより 5.0 出荷します。 回避策は下記の Workaround セクションで文書化されています。 Cisco は CCS 4.x バージョンからこの脆弱性を取除くために自動化されたスクリプトを提供しました

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040630-CCS で利用できます。

該当製品

修正済みソフトウェア

3.0E 以前の ServletExec パッチ設定されていないバージョンを使用して CCS は脆弱です。

- CCS 4.x は修正されるまで脆弱である ServletExec 3.0 と出荷します。 CCS 4.0 顧客は CCS 5.x に自動化されたスクリプトとのソフトウェアかアップグレードを修正できます。
- CCS 3.x は修正されるまで脆弱である ServletExec 2.2 と出荷します。 自動化されたスクリプトは CCS 3.0 に利用できません。 顧客は自動化されたスクリプトと Workaround セクションの手動手順に修正し、CCS 4.x にアップグレードし、CCS 5.x にソフトウェア従うことによってソフトウェアを、かアップグレードを修正できます。

脆弱性を含んでいないことが確認された製品

CCS 5.x は ServletExec 4.1 と出荷し、脆弱ではないです。

改訂履歴

リビジョン 1.0	2004-June-30	初回公開リリース

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。