Cisco Secure Desktop の多重 脆弱点

High	**アドバイザリーID :** cisco-sa-20061108-csd **初公開日 :** 2006-11-08 16:00 **バージョン 1.2 :** Final **CVSSスコア :** 7.0 **回避策 :** Yes **Cisco バグ ID :**	CVE-2006-5808 CVE-2006-5807 CVE-2006-5806

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 Secure Desktop （ CSD ）ソフトウェアはかもしれない 3 脆弱性から影響を受けます:

- SSL VPN セッション 終端の後でコンピュータで置き去りになるべきセッションを参照するインターネットの間に生成 され、アクセスされる情報を引き起こして下さい。
- ユーザをシステム ポリシーを避けることを許可して下さい防ぐ VPN 接続がアクティブな間、Secure Desktop を残すことを。
- ローカルユーザを特権を上げることを許可して下さい。

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。 利用可能 な 回避策がいくつかのこれらの脆弱性の効果を軽減するためにあります。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20061108-csd で掲示されます。

該当製品

修正済みソフトウェア

この文書に説明がある脆弱性は Cisco Secure Desktop のバージョン 3.1.1.33 および それ 以前にあります。

脆弱性を含んでいないことが確認された製品

Cisco Secure Desktop のバージョン 3.1.1.45 および それ 以降はこれら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 1.2	2007 年 2 月 21 日	「引き起こブラウザによる情報漏出」脆弱性（CSCsg05935）のための明白にされた回避策。
リビジョン 1.1	2006-November-08	iDefense アドバイザリへの含まれたリンク。
リビジョン 1.0	2006-November-08	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。