

Cisco Security Agent for Windows のシステム ドライバのリモート バッファ オーバーフロー脆弱性

Critical	アドバイザーID : cisco-sa-20071205-csa	CVE-2007-5580
	初公開日 : 2007-12-05 16:00	5580
	バージョン 1.2 : Final	CVE-2007-5582
	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

Cisco Security Agent for Microsoft Windows が使用するシステム ドライバには、バッファ オーバーフローの脆弱性が存在します。このバッファ オーバーフローはリモートで悪用でき、カーネルメモリを破壊し、それによって Windows 停止エラー (ブルー画面) や任意のコードの実行を可能にします。

この脆弱性は、TCP ポート 139 または 445 を宛先とする細工された TCP セグメントを処理する際に発生します。これらのポートは、Microsoft Server Message Block (SMB) プロトコルで使用されます。

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。

この脆弱性には、Common Vulnerabilities and Exposures (CVE) 識別子 CVE-2007-5580 が割り当てられています。

このアドバイザーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20071205-csa> で掲示されます。

該当製品

修正済みソフトウェア

すべてのバージョンの Cisco Security Agent for Windows (管理対象とスタンドアロンの両方

) が該当します。Cisco IP Communications アプリケーション サーバー上で実行されているエージェントや、Cisco Security Manager を実行しているシステム上のエージェントなどは、スタンドアロン実装の例です。

スタンドアロン エージェントは、次の Cisco IP Communications 製品にインストールされます。

- Cisco Unified Communications Manager (CallManager)
- Cisco Conference Connection (CCC)
- Emergency Responder
- IPCC Express
- IPCC Enterprise
- IPCC Hosted
- IP Interactive Voice Response (IP IVR)
- IP Queue Manager
- Intelligent Contact Management (ICM)
- Cisco Voice Portal (CVP)
- Cisco Unified Meeting Place
- Cisco Personal Assistant (PA)
- Cisco Unity
- Cisco Unity Connection
- Cisco Unity Bridge
- Cisco Internet Service Node (ISN)

Cisco Security Manager のインストール時にエージェントが検出されないと、Cisco Security Manager は Cisco Security Agent のスタンドアロン バージョンをインストールするので、Cisco Security Manager が稼働するシステムもこの脆弱性に該当します。

脆弱性を含んでいないことが確認された製品

Cisco Secure Access Control Server (ACS) Solution Engine (ACS アプライアンスとも呼ばれます) は、Cisco Security Agent のスタンドアロン バージョンを統合します。ただし、ACS Solution Engine は、該当する TCP ポート (139 と 445) に着信したトラフィックをデフォルトでブロックするので、この脆弱性には該当しません。詳細については、「[詳細情報](#)」セクションを参照してください。

Solaris および Linux オペレーティング システム上で稼働している Cisco Security Agent は、この脆弱性には該当しません。

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。

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	2008- April-25	CSCsI00618 のために記録する CVSS への更新済リンク。
リビジョン 1.1	2008- January -10	Cisco Unified Contact Center Express、Unity、Cisco Unified Contact Center Enterprise、Cisco Unified Contact Center Hosted および Intelligent Contact Management (ICM) のための追加された修正済みソフトウェア 情報。
リビジョン 1.0	2007 年 12 月 5 日	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。