# Cisco VPN Client IPSecドライバ カーネル メモリ不良脆弱性

| | | |
|---|---|---|
| Medium | **アドバイザリーID :** Cisco-SA-20080115-CVE-2008-0324<br>**初公開日 :** 2008-01-15 22:42<br>**バージョン 1.0 :** Final<br>**CVSSスコア :** 4.6<br>**回避策 :** Yes<br>**Cisco バグ ID :** | CVE-2008-0324 |

**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

Windows バージョン 5.0.02.0090 のための Cisco VPN Client はサービス拒否 （ DoS ）状態に終ってローカル攻撃者が影響を受けたシステムが失敗し、再起動しますことを可能にする可能性がある脆弱性が含まれています。

無効 な メモリ オペレーションによるこの脆弱性存在。 攻撃者は設計されているプログラムの実行によって影響を受けたアプリケーションに悪意のある要求をするようにこの脆弱性を不正利用する可能性があります。 従ってこれらの要求の処理の結果として、アプリケーションはシステムメモリを可能性がありま、失敗し、再起動するためにシステムを引き起こし破損する正規のユーザにサービスを否定します。

DoS 状態を示すプルーフ オブ コンセプト コード存在。

Cisco はこの脆弱性を確認しないし、更新は利用できません。

攻撃者は影響を受けたシステムに影響を受けたアプリケーションに悪意のある入力を入れるようにローカルでログオンし、設計されているプログラムを実行する必要があります。Â により工クスプロイト システムは DoS 状態に終って、失敗し、再起動します可能性があります。Â 存在 する証拠無しエクスプロイトに起因する任意 の コードを実行するのにメモリ不良が活用できることを示します。

thatÂ がエクスプロイトによって最も影響を与えることができるシステムはマルチユーザー システムです。VPN クライアント ソフトウェアが頻繁に専用またはシングルユーザ システムで展開

されるので Â は、DoS ローカルシステムの攻撃者か 1 人の他のユーザしか影響を与えないかもしれません。

### 該当製品

## 修正済みソフトウェア

Windows バージョン 5.0.02.0090 のための Cisco VPN Client は脆弱です。Â はまた他のバージョン影響を受けるかもしれません。

## 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

| バージョン | 説明 | Section | ステータス | 日付 |
|---|---|---|---|---|
| 1.0 | 初版リリース | 該当なし | Final | 2008-Jan-15 |

### 利用規約