# Cisco IP Phone Session Initiation Protocol（SIP）サービス拒否の脆弱性

| | | |
|---|---|---|
| Medium | **アドバイザリーID：** Cisco-SA-20070821-CVE-2007-4459<br>**初公開日：** 2007-08-21 20:30<br>**最終更新日：** 2012-07-14 20:02<br>**バージョン 2.0：** Final<br>**CVSSスコア：** 6.1<br>**回避策：** Yes<br>**Cisco バグ ID：** | CVE-2007-4459 |

**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

Voice VLAN の攻撃者が電話が失敗し、再起動しますことを可能にする可能性がある一連の SIP メッセージを処理するときファームウェアのバージョン 8.6 が付いている Cisco 7940 および 7960 の IP フォンはおよび前脆弱性が含まれています。

影響を受けたデバイスに送られる不正 な SIP メッセージのある特定のセットの不十分な処理によるこの脆弱性存在。Â は影響を受けたデバイスへ一連の悪意のある SIP メッセージを送信 することによって非認証、voice VLAN へのアクセスのリモート攻撃者この脆弱性を不正利用する可能性があります。デバイスがこれらのメッセージを処理するとき Â は、デバイス失敗し、再起動するかもしれません。Â はサービス拒否状態という結果にエクスプロイト終る可能性があります。

エクスプロイト コードは利用できます。

Cisco はこの脆弱性を確認し、更新済ソフトウェアは利用できます。

この脆弱性を不正利用するために、攻撃者は影響を受けたデバイスが取付けられるネットワークにアクセスできなければなりません。サイト設定による Â は別途の物理的かロジカルネットワークに、IP 電話常駐する可能性があります。Â はエクスプロイト 攻撃者がサービス拒否状態という結果に終るかもしれない影響を受けたデバイスを利用できないすることを可能にする可能性があります。しかし Â は機密 情報への、攻撃者アクセス権を得か、または不正侵入の成功の結果として追加特権を得ることができませんでした。

この脆弱性は状態管理不具合のようです。影響を受けたデバイスが SIP メッセージの特定のシーケンスに応答するとき Â は、電話デバイスの再度ブートするを引き起こすクラッシュという結果に終る可能性があるステート テーブルを破損するかもしれません。

このバージョンが訂正が含まれているので、ファームウェアのバージョン 8.7 を実行する Cisco 7940 および 7960 IP 電話はこの脆弱性から影響を受けません。

### 該当製品

## 修正済みソフトウェア

ファームウェア 8.6 が付いている Cisco 7940 および 7960 の IP フォンはおよび前脆弱です。

## 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

| 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 | 2007-Aug-21 |

### 利用規約