ARP 不正侵入からのアクセス ポイント メモリ枯渇

severity	**アドバイザリーID :** cisco-sa-20060112-wireless **初公開日 :** 2006-01-12 16:00 **バージョン 1.0 :** Final **回避策 :** Yes **Cisco バグ ID :**	CVE-2006-0354

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

悪意のあるユーザがデバイスがトラフィックを通過させることを止めるためにおよび/またはユーザ接続を破棄しますアクセス ポイントに IP アドレス 解決 プロトコル（ARP）によって巧妙に細工された 攻撃を送信 することを可能にするかもしれない IOS を実行する Cisco Aironet ワイヤレスアクセスポイント（AP）で存在 する脆弱性。

この脆弱性の繰り返された利用は支えられた DoS （サービス拒否）を作成します。

シスコでは、該当するお客様用に、こ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。 この脆弱性に対しては、影響を緩和するための回避策があります。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060112-wireless で掲示されます。

該当製品

修正済みソフトウェア

この Security Advisory はすべての Cisco Aironet に Cisco IOSソフトウェアを実行するワイヤレスアクセスポイントを加えます。 影響を受けたデバイスの種類は下記のものを含んでいます：

- Cisco Aironet 1400 シリーズ ワイヤレスブリッジ
- Cisco Aironet 1300 シリーズ アクセス ポイント
- Cisco Aironet 1240AG シリーズ アクセス ポイント

- Cisco Aironet 1230AG シリーズ アクセス アクセス・ポイント
- Cisco Aironet 1200 シリーズ Access Points
- Cisco Aironet 1130AG シリーズ アクセス ポイント
- Cisco Aironet 1100 シリーズ Access Points
- IOS を実行する Cisco Aironet 350 シリーズ アクセス ポイント

脆弱性を含んでいないことが確認された製品

VxWorks を実行する Ciscoワイヤレス デバイスは基づかせていましたイメージ（バージョン 12.05 および それ 以前）を

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 1.0	12-January-2006	初版リリース

利用規約