Cisco Airespace ワイヤレス LAN コントローラは非暗号化ネットワーク アクセスを許可します

severity	**アドバイザリーID :** cisco-sa-20051102-lwapp	CVE-2005-3482
	初公開日 : 2005-11-02 15:00	
	バージョン 1.0 : Final	
	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

Lightweight Access Point Protocol（LWAPP）モードで動作する Ciscoアクセスポイントは非認証エンドホストが既に認証されたエンドホストのメディア アクセス制御（MAC）アドレスからの帯の送信によってセキュア ネットワークに非暗号化トラフィックを送信 するようにするかもしれません。

LWAPP（別途のワイヤレス LAN コントローラによってすなわち、制御されて）モードでオペレーティングのアクセス ポイントだけ影響を受けています。 自律モードで動作しているアクセス ポイントは影響を受けていません。

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。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20051102-lwapp で掲示されます。

該当製品

修正済みソフトウェア

Cisco 1200、1131、および Cisco 2000 および 4400 シリーズ Airespace Wireless LAN（WLAN）コントローラが制御するソフトウェア バージョン 3.1.59.24 を実行している 1240 シリーズ アクセス ポイントはこの脆弱性から影響を受けます。

この問題は別途の WLAN コントローラの配備にだけ適当です。 別途の WLAN コントローラの

ないどのシステムでも脆弱ではないです。

脆弱性を含んでいないことが確認された製品

脆弱性を含んでいない製品は次のとおりです。

- Cisco 1200 以外のアクセス ポイントは、1131 および 1240 シリーズ影響を受けていません。
- 別途の WLAN コントローラなしで配置されるアクセス ポイントは影響を受けていません。
- Cisco 2000 および 4400 シリーズ以外 WLAN コントローラによって制御されるアクセス ポイントは影響を受けていません。
- 3.1.59.24 以外ソフトウェア バージョンを実行している WLAN コントローラによって制御されるアクセス ポイントは影響を受けていません。
- 自律モードで動作しているアクセス ポイントは影響を受けていません。
- VxWorks を実行しているアクセス ポイントは影響を受けていません。

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 1.0	2005-Nov-2	初版リリース

利用規約