WLSE アプライアンスの多重 脆弱点

severity	**アドバイザリーID :** cisco-sa-20060419-wlse	CVE-2006-1960
	初公開日 : 2006-04-19 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

CiscoWorks ワイヤレス LAN ソリューション エンジン（WLSE）にある 2 脆弱性があります。第 1 は攻撃者がシステムの管理権限を得ることを可能にするかもしれないクロスサイト スクリプティング（XSS）脆弱性です。 第 2 は基礎オペレーティング システムにアクセスを得るコマンド ライン インターフェースに既に許可されたアクセスをアクセスできている攻撃者によって使用できるローカル特権 拡大脆弱性です。

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。

このアドバイザリは 419-wlse で利用できます

該当製品

修正済みソフトウェア

2.13 前にソフトウェアのバージョンを実行する CiscoWorks ワイヤレス LAN ソリューション エンジン（WLSE）か WLSE Express は両方の脆弱性に脆弱です。

複数のその他のCisco製品は Cisco Hosting Solution Engine （HSE）、ユーザ登録ツール（URT）、Cisco Ethernet Subscriber Solution Engine （ESSE）および CiscoWorks2000 Service Management Solution を含むローカル特権 拡大脆弱性からだけ、影響を受けます。 別途の Ciscoセキュリティ応答はこれらの製品の影響および修正に関して送達され、419-priv で見つけることができます

脆弱性を含んでいないことが確認された製品

その他のCisco製品は両方の脆弱性から影響を受けません。

改訂履歴

リビジョン 1.0	2006-April-19	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、単独の転載や意訳を施した場合、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。