

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)[Security Advisories](#)

# Cisco Security Advisory: Multiple Vulnerabilities in the WLSE Appliance

Advisory ID: cisco-sa-20060419-wlse

<http://www.cisco.com/warp/public/707/cisco-sa-20060419-wlse.shtml>

## Revision 1.0

For Public Release 2006 April 19 1500 UTC (GMT)

---

Please provide your [feedback](#) on this document.

---

## Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Impact](#)
- [Software Version and Fixes](#)
- [Workarounds](#)
- [Obtaining Fixed Software](#)
- [Exploitation and Public Announcements](#)
- [Status of this Notice: FINAL](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

---

## Summary

There are two vulnerabilities that exist in the CiscoWorks Wireless LAN Solution Engine (WLSE). The first is a cross site scripting (XSS) vulnerability that may allow an attacker to gain administrative privileges on the system. The second is a local privilege escalation vulnerability that can be used by an attacker who already has authenticated access to the command line interface to obtain access to the underlying operating system.

Cisco has made free [software](#) available to address this vulnerability for affected customers.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20060419-wlse.shtml>

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

## ☐ Affected Products

This section provides details on affected products.

### ☐ Vulnerable Products

A CiscoWorks Wireless LAN Solution Engine (WLSE) or WLSE Express running any version of software prior to 2.13 are vulnerable to both of these vulnerabilities.

Several other Cisco products are affected only by the local privilege escalation vulnerability, including Cisco Hosting Solution Engine (HSE), User Registration Tool (URT), Cisco Ethernet Subscriber Solution Engine (ESSE) and CiscoWorks2000 Service Management Solution. A separate Cisco Security Response has been published regarding the impact and the fixes on these products and can be found at <http://www.cisco.com/warp/public/707/cisco-sr-20060419-priv.shtml>

### ☐ Products Confirmed Not Vulnerable

No other Cisco products are affected by both of these vulnerabilities.

[Top of the section](#) [Close Section](#)

## ☐ Details

CiscoWorks WLSE is a centralized, systems-level application for managing and controlling an entire autonomous Cisco WLAN infrastructure.

Two vulnerabilities exist in the WLSE appliance that may allow an attacker to gain complete control of the device or to obtain access to the underlying operating system.

These issues are documented by the following Cisco bug IDs:

- [CSCsc01095](#) ([registered](#) customers only) - Cross site scripting vulnerability in WLSE appliance web interface  
This fix addresses the cross site scripting (XSS) vulnerability in the WLSE appliance web user interface. By exploiting this vulnerability, an attacker may obtain the session cookie information and further use this information to gain administrative privileges on the system.
- [CSCsd21502](#) ([registered](#) customers only) - Privilege escalation to Linux shell  
This fix addresses the local privilege escalation from the command line interface of the WLSE appliance. By exploiting this vulnerability an attacker who already has authenticated access to the command line interface may inject a command to obtain a shell account on the underlying operating system.

[Top of the section](#) [Close Section](#)

## ☐ Impact

By exploiting these vulnerabilities together, an attacker may obtain complete control of the WLSE appliance.

[Top of the section](#)   [Close Section](#)

## ☐ Software Version and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

These vulnerabilities are fixed in the 2.13 version of WLSE software. Fixed software can be downloaded from the following URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/wlan-sol-eng>

[Top of the section](#)   [Close Section](#)

## ☐ Workarounds

There are no workarounds for these vulnerabilities.

[Top of the section](#)   [Close Section](#)

## ☐ Obtaining Fixed Software

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

[Top of the section](#)   [Close Section](#)

## ☐ Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

[Top of the section](#)   [Close Section](#)

## ☐ Customers using Third Party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

[Top of the section](#)   [Close Section](#)

## ☐ Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: [tac@cisco.com](mailto:tac@cisco.com)

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

[Top of the section](#)   [Close Section](#)

## ☐ Exploitation and Public Announcements

The Cisco PSIRT is not aware of malicious use of the vulnerability described in this advisory.

This vulnerability was reported to Cisco by Adam Pointon of Assurance.Com.Au. We would like to thank Adam Pointon for bringing this to our attention.

[Top of the section](#)   [Close Section](#)

## ☐ Status of this Notice: FINAL

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

[Top of the section](#)   [Close Section](#)

## ☐ Distribution

This advisory is posted on Cisco's worldwide website at :

<http://www.cisco.com/warp/public/707/cisco-sa-20060419-wlse.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- [cust-security-announce@cisco.com](mailto:cust-security-announce@cisco.com)
- [first-teams@first.org](mailto:first-teams@first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto:comp.dcom.sys.cisco@newsgate.cisco.com)

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

[Top of the section](#)   [Close Section](#)

## ☐ Revision History

Revision 1.0	2006-April-19	Initial public release.
--------------	---------------	-------------------------

[Top of the section](#)   [Close Section](#)

## ☐ Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html). This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

[Top of the section](#)   [Close Section](#)

**Help us help you.**

**Please rate this document.**

- Excellent
- Good
- Average
- Fair
- Poor

**This document solved my problem.**

- Yes
- No
- Just browsing

**Suggestions for improvement:**

(256 character limit)

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)