

Cisco Security Advisory: Cisco Airespace Wireless LAN Controllers Allow Unencrypted Network Access

Advisory ID: cisco-sa-20051102-lwapp

<http://www.cisco.com/warp/public/707/cisco-sa-20051102-lwapp.shtml>

Revision 1.0

For Public Release 2005 November 02 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

Cisco Access Points operating in Lightweight Access Point Protocol (LWAPP) mode may allow unauthenticated end hosts to send unencrypted traffic to a secure network by sending frames from the Media Access Control (MAC) address of an already authenticated end host.

Only the access points that are operating in LWAPP (i.e., controlled by a separate Wireless LAN

Controller) mode are affected. Access points that are running in autonomous mode are not affected.

Cisco has made free software available to address this vulnerability for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051102-lwapp.shtml>.

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

☐ **Affected Products**

This section provides details on affected products.

☐ **Vulnerable Products**

Cisco 1200, 1131, and 1240 series access points controlled by Cisco 2000 and 4400 series Airespace Wireless LAN (WLAN) Controllers that are running software version 3.1.59.24 are affected by this vulnerability.

This issue is only applicable to deployments where there is a separate WLAN controller. Any system without a separate WLAN controller is not vulnerable.

☐ **Products Confirmed Not Vulnerable**

These products are not vulnerable:

- Access points other than Cisco 1200, 1131 and 1240 series are not affected.
- Access points that are deployed without a separate WLAN controller are not affected.
- Access points that are controlled by WLAN controllers other than Cisco 2000 and 4400 series are not affected.
- Access points that are controlled by WLAN controllers which are running a software version other than 3.1.59.24 are not affected.
- Access points that are running in autonomous mode are not affected.
- Access points that are running VxWorks are not affected.

No other Cisco products are currently known to be affected by these vulnerabilities.

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

☐ **Details**

LWAPP is an open protocol for access point management. In this mode of operation, a WLAN controller system is used to create and enforce policies across multiple different lightweight access points. All functions essential to WLAN operations are centrally controlled by WLAN controllers. In this mode of operation, Cisco access points run a simplified version of Cisco IOS®. It is not possible to enter into configuration mode and configure access points individually in this mode. More information on LWAPP mode of operation can be found at the following URL:

http://www.cisco.com/en/US/products/ps6306/prod_white_papers_list.html

A Cisco access point running in LWAPP mode can be checked by issuing the following command from the console.

```
configure terminal
```

Access points running in LWAPP mode will not allow the user to enter into configuration mode, but will return an error message instead as shown in the following output.

```
AP000e.8466.5786>enable  
AP000e.8466.5786#configure terminal  
      ^  
% Invalid input detected at '^' marker.  
  
AP000e.8466.5786#
```

The alternative to LWAPP mode is the autonomous mode of operation. In this mode, the access points are configured individually and run either VxWorks or Cisco IOS operating systems.

Cisco 1200, 1131 and 1240 series access points that are controlled by 2000 or 4400 WLAN controllers in LWAPP mode of operation may accept unencrypted traffic from end hosts even when configured to encrypt traffic. Such traffic needs to be sourced from the MAC address of a legitimate, already authenticated end host. By exploiting this vulnerability, an attacker may send malicious traffic into a secure network. Legitimate end hosts will still communicate with the access point in an encrypted manner.

Only the access points that are running in LWAPP mode are affected by this vulnerability. Access points that are running in autonomous mode are not affected.

In LWAPP mode, access points download their software from the WLAN controller. Therefore, a software upgrade on the WLAN controller is required to address this vulnerability.

This issue is documented by the Cisco bug ID [CSCsc11134](#) ([registered](#) customers only) .

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

☐ **Impact**

Successful exploitation of the vulnerability may allow an attacker to send malicious traffic to a secure wireless network via an access point that is controlled by an affected WLAN controller.

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

☐ **Software Version and Fixes**

When considering software upgrades, please also consult http://www.cisco.com/en/US/products/products_security_advisories_listing.html 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") for assistance.

In LWAPP mode of operation, it is not possible to change the software on the access points individually. Access points download their software from the WLAN controller. Therefore, a software upgrade on the WLAN controller is required. This issue is fixed in version 3.1.105.0 of WLAN controller software.

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

☐ Workarounds

There are no workarounds for this issue.

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

☐ Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. 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 the following URLs.

- http://www.cisco.com/cgi-bin/tablebuild.pl/2000_series_Wireless_LAN_controller for Cisco 2000 Series WLAN Controller
- http://www.cisco.com/cgi-bin/tablebuild.pl/4400_series_Wireless_LAN_controller for Cisco 4400 Series WLAN Controller

[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 assistance with the upgrade, which should be free of charge.

[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

Please 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.

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

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>.

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

☐ Exploitation and Public Announcements

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

[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-20051102-lwapp.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
- first-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- 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	2005-Nov-2	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. 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](#)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

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

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)