

Cisco Security Advisory: Multiple Vulnerabilities in the Cisco Wireless LAN Controller and Cisco Lightweight Access Points

Advisory ID: cisco-sa-20070412-wlc

<http://www.cisco.com/warp/public/707/cisco-sa-20070412-wlc.shtml>

Revision 1.4

Last Updated 2008 April 24 2120 UTC (GMT)

For Public Release 2007 April 12 1600 UTC (GMT)

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

Contents

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

Summary

The Cisco Wireless LAN Controller (WLC) manages Cisco Aironet access points using the Lightweight Access Point Protocol (LWAPP). The WLC contains multiple vulnerabilities that could result in a denial of service (DoS) condition, information disclosure, or access control list changes, or allow an attacker to

gain full administrative access.

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070412-wlc.shtml>.

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

☐ **Affected Products**

☐ **Vulnerable Products**

Vulnerable Software

The vulnerabilities addressed in this document affect versions 4.0, 3.2, and prior versions of the Wireless LAN Controller software. To identify the first fixed version for a specific Cisco Bug ID, please see the Software Versions and Fixes section of this advisory.

To determine the version of WLC running in a given environment, use one of the following methods:

- In the web interface, choose the **Monitor** tab, click **Summary** in the left-hand pane, and note the "Software Version."
- From the command-line interface, type **show sysinfo** and note the "Product Version."

Vulnerable Hardware

Wireless LAN Controllers

- Cisco 4400 Series Wireless LAN Controllers
- Cisco 4100 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 2000 Series Wireless LAN Controllers
- Cisco Wireless LAN Controller Module

Wireless Integrated Switches and Routers

- Cisco Catalyst 6500 Series Wireless Services Module (WiSM)
- Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers
- Cisco Wireless LAN Controller Module

Cisco Aironet Access Points

- Cisco Aironet 1000 Series
- Cisco Aironet 1500 Series

☐ **Products Confirmed Not Vulnerable**

- Cisco Aironet 1400 Series
- Cisco Aironet 1300 Series
- Cisco Aironet 1240 AG Series
- Cisco Aironet 1230 AG Series
- Cisco Aironet 1200 Series
- Cisco Aironet 1130 AG Series
- Cisco Aironet 1100 Series

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

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

▣ Details

The Cisco Wireless LAN Controller (WLC) manages Cisco Aironet access points using the Lightweight Access Point Protocol (LWAPP). This protocol provides centralized management of wireless networks. The WLC contains the following vulnerabilities:

Default SNMP Community Strings

The WLC uses the commonly known values of "public" and "private" for its read-only and read-write SNMP community strings. This vulnerability is documented by Cisco Bug ID [CSCse02384](#) ([registered](#) customers only) .

Malformed Ethernet Traffic Crash

The WLC may crash in response to malformed Ethernet traffic. This vulnerability is documented by Cisco Bug ID [CSCsc90179](#) ([registered](#) customers only) .

Multiple NPU Lock-Up Vulnerabilities

The Network Processing Unit (NPU) is responsible for handling traffic within the WLC. It is possible to cause one or more NPUs to lock up by sending certain types of traffic to an affected WLC. This traffic includes crafted SNAP packets, malformed 802.11 traffic, and packets with unexpected length values in certain headers.

Each NPU operates independently and serves two of the physical ports on the WLC. A lock up in one NPU does not affect the others, so the number of NPUs available and the configuration of the device determine whether these vulnerabilities result in a partial or complete inability to forward traffic. To clear a NPU lock up, the WLC must be restarted. If the lock up condition prevents access to the management interface, the restart must be performed via the console port or service port.

Devices that implement the WLC functionality in software rather than hardware do not contain a NPU and are not affected by these vulnerabilities. These software-based devices are the 2000 Series WLC, the 2100 Series WLC, and the Cisco Wireless LAN Controller Module.

These vulnerabilities are documented by Cisco Bug IDs [CSCsg36361](#) ([registered](#) customers only) , [CSCsg15901](#) ([registered](#) customers only) , and [CSCsh10841](#) ([registered](#) customers only) .

Hard-Coded Service Password in Lightweight AP

The Cisco Aironet 1000 Series and 1500 Series Lightweight Access Points contain a hard-coded service password that is used for troubleshooting. This service account is only accessible via a physical connection to the console port, but the password is common to all units in these series. This vulnerability is documented by Cisco Bug ID [CSCsg15192](#) ([registered](#) customers only) .

WLAN ACL Does Not Persist Through Reboot

Version 4.0 of the WLC contains a bug when processing WLAN ACLs that causes the WLAN ACL configuration to be saved with an invalid checksum. This bug does not affect 3.2 versions of the WLC. When the configuration is subsequently reloaded at boot time, the checksum fails and the WLAN ACLs are not installed. This vulnerability is documented by Cisco Bug ID [CSCse58195](#) ([registered](#) customers only) .

Vulnerability Scoring Details

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS).

Cisco will provide a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias parameter when determining the environmental impact of a particular vulnerability.

CVSS is a standards based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided an FAQ to answer additional questions regarding CVSS at <http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at <http://intellishield.cisco.com/security/alertmanager/cvss>.

CSCse02384 (registered customers only)						
Calculate the environmental score of CSCse02384 ↗						
CVSS Base Score - 10						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Complete	Complete	Complete	Normal
CVSS Temporal Score - 8.3						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

[CSCsc90179](#) (**registered** customers only)

Calculate the environmental score of [CSCsc90179](#) 

CVSS Base Score - 3.3

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal

CVSS Temporal Score - 2.7

Exploitability	Remediation Level	Report Confidence
Functional	Official Fix	Confirmed

[CSCsg36361](#) (**registered** customers only)

Calculate the environmental score of [CSCsg36361](#) 

CVSS Base Score - 3.3

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal

CVSS Temporal Score - 2.7

Exploitability	Remediation Level	Report Confidence
Functional	Official Fix	Confirmed

[CSCsg15901](#) (**registered** customers only)

Calculate the environmental score of [CSCsg15901](#) 

CVSS Base Score - 3.3

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal

CVSS Temporal Score - 2.7

Exploitability	Remediation Level	Report Confidence
Functional	Official Fix	Confirmed

[CSCsh10841](#) (**registered** customers only)

Calculate the environmental score of [CSCsh10841](#) 

CVSS Base Score - 3.3

Access	Access		Confidentiality	Integrity	Availability	Impact
--------	--------	--	-----------------	-----------	--------------	--------

Vector	Complexity	Authentication	Impact	Impact	Impact	Bias
Remote	Low	Not Required	None	None	Complete	Normal
CVSS Temporal Score - 2.7						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

CSCsg15192 (registered customers only)						
Calculate the environmental score of CSCsg15192 ↗						
CVSS Base Score - 5.6						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Local	High	Not Required	Complete	Complete	Complete	Normal
CVSS Temporal Score - 4.6						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

CSCse58195 (registered customers only)						
Calculate the environmental score of CSCse58195 ↗						
CVSS Base Score - 3.7						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	High	Not Required	Partial	Partial	None	Normal
CVSS Temporal Score - 3.1						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

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

☐ Impact

Successful exploitation of these vulnerabilities may result in the issues described in this section.

Default SNMP Community Strings

CSCse02384: This vulnerability allows authenticated, remote attackers to utilize common credentials to read and modify the configuration of the WLC via SNMP.

Malformed Ethernet Traffic Crash

CSCsc90179: This vulnerability may allow unauthenticated attackers on a local network segment to crash the WLC, resulting in a DoS condition.

Multiple NPU Lock-Up Vulnerabilities

CSCsg36361: This vulnerability allows unauthenticated attackers on a local wireless network segment to prevent the WLC from passing traffic, resulting in either a partial or complete DoS condition.

CSCsg15901: This vulnerability allows unauthenticated attackers on a local wireless network segment to prevent the WLC from passing traffic, resulting in either a partial or complete DoS condition.

CSCsh10841: This vulnerability allows unauthenticated attackers on a local wireless network segment to prevent the WLC from passing traffic, resulting in either a partial or complete DoS condition.

Hard-Coded Service Password in Lightweight AP

CSCsg15192: This vulnerability allows an attacker with physical access to take control of an affected lightweight access point.

WLAN ACL Does Not Persist Through Reboot

CSCse58195: This vulnerability causes the WLAN ACL configuration to be disregarded, resulting in a silent and unexpected change to the security posture of a wireless network.

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

☐ Software Versions 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.

Each row of the software table (below) describes the earliest software version that contains the fix (the "First Fixed Release") and the anticipated date of availability when fixes are not available. A device running a version that is earlier than the First Fixed Release is known to be vulnerable. The release should be upgraded at least to the indicated version (greater than or equal to the First Fixed Release label).

Cisco Bug ID	First Fixed Releases
--------------	----------------------

CSCse02384	4.1.171.0
CSCsc90179	3.2.116.21, 4.0.155.0
CSCsg36361	3.2.193.5, 4.0.206.0, 4.1.171.0
CSCsg15901	3.2.171.5, 4.0.206.0, 4.1.171.0
CSCsh10841	3.2.171.5, 4.0.206.0, 4.1.171.0
CSCsg15192	3.2.185.0, 4.0.206.0
CSCse58195	4.0.206.0

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

☐ Workarounds

This section describes workarounds for these vulnerabilities.

Default SNMP Community Strings

Customers can mitigate this vulnerability by changing the SNMP community strings from their default values. This can be accomplished on each WLC by using the menu to access **Management > SNMP > Communities** and then changing the values of the community strings. On larger networks, the Cisco Wireless Control System can be used to apply SNMP changes across multiple controllers simultaneously.

Malformed Ethernet Traffic Crash

There are no known workarounds for this vulnerability.

Multiple NPU Lock-Up Vulnerabilities

There are no known workarounds for these vulnerabilities.

Hard-Coded Service Password in Lightweight AP

There are no known workarounds for this vulnerability.

WLAN ACL Does Not Persist Through Reboot

There are no known workarounds for this vulnerability.

Additional Workarounds

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory:

<http://www.cisco.com/warp/public/707/cisco-amb-20070412-wlc.shtml>

[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 <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

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 any public announcements or malicious use of the vulnerabilities described in this advisory.

These vulnerabilities were discovered via internal testing and during the investigation of customer support cases.

[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-20070412-wlc.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
- 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 1.4	2008- April- 24	Updated links to the CVSS scoring for each bug ID.
Revision 1.3	2007- May- 16	Updated First Fixed Releases information to include the recent 4.1 software release.
Revision 1.2	2007- April- 16	Added additional products to the Wireless LAN Controller affected products and added information to the WLAN ACL Does Not Persist Through Reboot section.
Revision 1.1	2007- April- 14	Minor grammatical changes.
Revision 1.0	2007- April- 12	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](#)

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)

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

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

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