

Cisco Security Advisory: Multiple Vulnerabilities in the Cisco Wireless Control System

Advisory ID: cisco-sa-20070412-wcs

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

Revision 1.1

Last Updated 2007 April 14 0000 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 Control System (WCS) works in conjunction with Cisco Aironet Lightweight Access Points, Cisco Wireless LAN Controllers, and the Cisco Wireless Location Appliance by providing tools for wireless LAN planning and design, system configuration, location tracking, security

monitoring, and wireless LAN management. Cisco WCS contains multiple vulnerabilities that can result in information disclosure, privilege escalation, and unauthorized access through fixed authentication credentials.

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

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

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

☐ **Affected Products**

☐ **Vulnerable Products**

Versions of WCS prior to 4.0.96.0 are affected by one or more of these vulnerabilities. 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 WCS running in a given environment, take the following steps:

1. Log in to the WCS graphical web interface.
2. From the menu, select **Help > About the Software**.

☐ **Products Confirmed Not Vulnerable**

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

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

☐ **Details**

The Cisco Wireless Control System (WCS) works in conjunction with Cisco Aironet Lightweight Access Points, Cisco Wireless LAN Controllers, and the Cisco Wireless Location Appliance by providing tools for wireless LAN planning and design, system configuration, location tracking, security monitoring, and wireless LAN management. Cisco WCS contains the following vulnerabilities:

Fixed FTP Credentials For WCS Location Backup

WCS can be configured to back up the data stored on the Cisco Wireless Location Appliance via FTP. Affected versions of WCS include a fixed user name and password for this backup operation; these credentials cannot be changed or disabled. Knowledge of these credentials, when combined with other properties of the FTP server, could allow an attacker to read from and write to arbitrary files on the server hosting the WCS application. In some cases, this could be leveraged to alter system files and compromise the server. This vulnerability is documented by Cisco Bug ID [CSCse93014](#) ([registered](#) customers only) .

Account Group Privilege Escalation

The WCS authentication system contains a privilege escalation vulnerability that allows any user with a valid user name and password to change their account group membership. For example, a user in the "LobbyAmbassador" group can add themselves to the "SuperUsers" group. This privilege escalation can allow full administrative control of WCS and the wireless networks it manages. This vulnerability is documented by Cisco Bug IDs [CSCse78596](#) and [CSCsg05190](#) ([registered](#) customers only) .

Information Disclosure to Unauthenticated Users

On affected versions of WCS, several directories within the WCS page hierarchy are not password protected and could be accessed by an unauthenticated user. Although the information available would not allow an attacker to gain access to WCS, it would be possible to obtain information about the organization of the network, including access point locations. This vulnerability is documented by Cisco Bug ID [CSCsg04301](#) ([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>.

CSCse93014 (registered customers only)						
Calculate the environmental score of CSCse93014 ↗						
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		

[CSCse78596](#) ([registered](#) customers only)

Calculate the environmental score of [CSCse78596](#) ↗

CVSS Base Score - 2.8						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Required	Partial	Partial	None	Normal
CVSS Temporal Score - 2.3						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

[CSCsg05190](#) ([registered](#) customers only)

Calculate the environmental score of [CSCsg05190](#) ↗

CVSS Base Score - 6						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Required	Complete	Complete	Complete	Normal
CVSS Temporal Score - 5						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

[CSCsg04301](#) ([registered](#) customers only)

Calculate the environmental score of [CSCsg04301](#) ↗

CVSS Base Score - 2.3						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Partial	None	None	Normal
CVSS Temporal Score - 1.9						
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.

Fixed FTP Credentials for WCS Location Backup

CSCse93014: This vulnerability allows an authenticated attacker to utilize fixed credentials to read from and write to arbitrary files on the server hosting the WCS application. In some cases, the attacker could leverage this ability to gain privileged access to the host.

Account Group Privilege Escalation

CSCse78596: This vulnerability allows an authenticated attacker with a valid user account to access information from any WCS configuration page.

CSCsg05190: This vulnerability allows an authenticated attacker with a valid user account to escalate their privileges to the SuperUsers group.

Information Disclosure to Unauthenticated Users

CSCsg04301: This vulnerability allows an unauthenticated attacker to obtain reconnaissance information from an affected system.

[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).

Note: Customers who currently run Cisco WCS 3.x are strongly encouraged to obtain a PAK certificate before they begin the upgrade process. For more information, please read the information under [Special Note for Customers Upgrading to Cisco WCS Release 4.0](#).

Cisco Bug ID	First Fixed Release
CSCse93014	4.0.96.0
CSCse78596	4.0.81.0
CSCsg05190	4.0.87.0
CSCsg04301	4.0.66.0

Special Note for Customers Upgrading to Cisco WCS Release 4.0

To request a PAK certificate to upgrade customers or partners from a previous release of Cisco WCS to Release 4.0, contact the wcs-customer-license@cisco.com. Cisco will attempt to respond to requests to this alias within 48 hours Monday-Friday 9AM-5PM Pacific.

Note: This alias is only for issuing PAK certificates for Cisco WCS license upgrades. It is not for requesting TAC support, troubleshooting, ordering issues, or customer service issues.

Please include in the email to request the PAK certificate:

- Customer name
- Customer email
- Company name
- Exact Cisco WCS SKUs to be upgraded
- Quantity of each Cisco WCS SKU
- Cisco sales order number
- Service contract number (SAU/SASU)

For Technical Support Related to Licensing-Contact Cisco TAC at (800) 553-2447 tac@cisco.com.

For Licensing Order Related Issues-Contact Cisco customer service at <http://www.cisco.com/go/customerservice>.

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

☐ Workarounds

This section describes workarounds for these vulnerabilities.

Fixed FTP Credentials for WCS Location Backup

There are no known workarounds for this vulnerability.

Account Group Privilege Escalation

As a workaround, customers can remove the accounts of users who access Cisco WCS from high-risk locations such as publicly accessible building lobbies.

Information Disclosure to Unauthenticated Users

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-wcs.shtml>

☐ **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.

☐ **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>.

☐ **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.

☐ **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-wcs.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 1.1	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)



Send

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

All contents are Copyright © 2006-2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).