

Cisco Security Advisory: Cisco Wireless Control System Conversion Utility Adds Default Password

Advisory ID: cisco-sa-20071010-wcs

<http://www.cisco.com/warp/public/707/cisco-sa-20071010-wcs.shtml>

Revision 1.1

Last Updated 2008 April 25 1430 UTC (GMT)

For Public Release 2007 October 10 1600 UTC (GMT)

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

Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Vulnerability Scoring 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

Customers who use the CiscoWorks Wireless LAN Solution Engine (WLSE) may use a conversion utility to convert over to a Cisco Wireless Control System (WCS). This conversion utility creates and

uses administrative accounts with default credentials. Because there is no requirement to change these credentials during the conversion process, an attacker may be able to leverage the accounts that have default credentials to take full administrative control of the WCS after the conversion has been completed.

Customers who have converted their CiscoWorks WLSE to a Cisco WCS are advised to set strong passwords for all accounts on their Cisco WCS.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20071010-wcs.shtml>.

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

☐ **Affected Products**

☐ **Vulnerable Products**

Cisco WCS systems that have been converted from a CiscoWorks WLSE using the conversion utility for version 4.1.91.0 or earlier are vulnerable.

☐ **Products Confirmed Not Vulnerable**

Cisco WCS systems that have not been converted from a CiscoWorks WLSE using the conversion utility are not affected by this problem. Additionally, Cisco WCS systems that have been converted from a CiscoWorks WLSE using the conversion utility for version 4.2 or later are not vulnerable.

For more information about Cisco Unified Wireless Network Software Release 4.2, visit:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6973/ps8382/prod_bulletin0900a

No other Cisco products are currently known to be affected by this vulnerability.

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

☐ **Details**

CiscoWorks WLSE is a centralized, systems-level application for managing and controlling an entire autonomous Cisco wireless LAN (WLAN) infrastructure. The Cisco Wireless Control System (WCS) is a centralized, systems-level application for managing and controlling lightweight access points and wireless LAN controllers for the Cisco Unified Wireless Network.

A CiscoWorks WLSE can be converted to a Cisco WCS using a utility that can be ordered from Cisco. There are two administrative accounts on the Wireless Control System (WCS): a Linux root account and Cisco WCS root account. Vulnerable versions of the conversion utility do not force the administrator to change the password for the Linux "root" user of the newly converted system. Non-vulnerable versions of the conversion utility force the administrator to change both account passwords.

More information about the conversion utility is available in the [Conversion of a WLSE Autonomous Deployment to a WCS Controller Deployment](#) appendix in the Cisco Wireless Control System Configuration Guide.

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

▣ Vulnerability Scoring Details

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

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.

Cisco has provided a 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>.

CSCsj71081 - Need to have installer on WLSE-WCS conversion procedures					
Calculate the environmental score of CSCsj71081 					
CVSS Base Score - 10.0					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - 8.3					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

▣ Impact

Successful exploitation of the vulnerability may result in full administrative control of the Cisco WCS system or user-level access to the host Linux operating system.

☐ **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.

☐ **Workarounds**

The vulnerability described in this document can be eliminated by logging in to the affected WCS and changing the default password for the administrative Linux root account to a strong password chosen by the user.

Refer to the [Managing User Accounts](#) chapter of the Cisco Wireless Control System Configuration Guide for more information about changing administrative accounts.

☐ **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.

Because the fix for this vulnerability is a default configuration change, and a workaround is available, a software upgrade is not required to address this vulnerability. However, if you have a service contract, and would like to upgrade to unaffected code, you may obtain upgraded software through your regular update channels when that software is available. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide web site at <http://www.cisco.com>.

☐ 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 vulnerability described in this advisory.

☐ **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.

☐ **Distribution**

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


<http://www.cisco.com/warp/public/707/cisco-sa-20071010-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.

☐ **Revision History**

Revision 1.1	2008-April-25	Updated link to the CVSS score of CSCsj71081  .
Revision 1.0	2007-October-10	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](#)

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