

Cisco Security Advisory: Default Password in Wireless Location Appliance

Document ID: 71780

Advisory ID: cisco-sa-20061012-wla

<http://www.cisco.com/warp/public/707/cisco-sa-20061012-wla.shtml>

Revision 1.0

For Public Release 2006 October 12 1600 UTC (GMT)

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

[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

The Cisco Wireless Location Appliance software contains a default password for the 'root' administrative account. A user who logs in using this username has complete control of the device.

This password is the same in all installations of the product prior to version 2.1.34.0 when shipped as part of a new product purchase. This vulnerability still exists on upgraded installations unless explicit steps have been taken to change the password after the initial installation of the product.

There are workarounds available for this vulnerability.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20061012-wla.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

This vulnerability affects Cisco 2700 Series Wireless Location Appliances shipped with versions prior to 2.1.34.0.

The version of software on the Wireless Location Appliance can be determined in one of three ways.

From the command line the version can be determined with the **getserverinfo** command. The version is contained in the first five lines of output which will look similar to the following output from a device running version 1.1.73.0:

```
-----  
Server Config  
-----  
Product name: Cisco Wireless Location Appliance  
Version: 1.1.73.0
```

Another way to get the version from the command line is to view the file /opt/locserver/conf/version.txt. For a WLA running version 2.0.42.0, the contents of that file should be similar to:

```
[root@locserv /]# cat /opt/locserver/conf/version.txt  
#Tue Jan 31 11:08:35 PST 2006  
build.number=42  
minor.number=0  
patch.number=0  
major.number=2  
branch.name=HOT  
product.name=Cisco Wireless Location Appliance
```

The version is simply obtained by assembling the numbers beginning with the "major.number" followed by "minor.number", "build.number" and "patch.number" in that order with each number separated by a period.

Lastly, the version may be obtained via the web interface on a Cisco Wireless Control System (WCS) for any Location Appliances which are configured on it. Browsing to the "Locations" tab and clicking on "Location Servers" in the resulting menu will give a list of Location Appliances with their corresponding versions under the "Versions" column.

Products Confirmed Not Vulnerable

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

Details

The Cisco Wireless Location Appliance (WLA) uses RF fingerprinting technology to simultaneously track 802.11 wireless devices from directly within a WLAN infrastructure. By design, the Cisco Wireless Location Appliance is directly integrated into the WLAN infrastructure using Cisco wireless LAN controllers and Cisco Aironet lightweight access points to track the physical location of wireless devices.

The Cisco Wireless Location Appliance can be managed via a virtual terminal (standard keyboard and monitor attached directly to the appliance), a local serial console, remote SSH connections, and/or remote secure web sessions. A special administrative account is provided so that certain management, troubleshooting tasks, and basic initial setup can be performed.

The default username for administrator login is "root" (without the quotes), and the default password is "password" (without the quotes). Both the username and password are case sensitive.

This issue has been addressed in fixed versions of software by prompting the user to change the password on the root account during the appliance setup installation. This only applies to new WLA devices shipped initially with a non-vulnerable version of software for the initial installation. Previous versions of software which have been upgraded will not prompt the user to change the password for the root user during the upgrade.

This issue is documented in Cisco Bug ID [CSCsb92893](#) ([registered](#) customers only) .

Impact

Successful exploitation of the vulnerability may result in a remote attacker gaining full administrative control of the device.

Software Version and Fixes

This vulnerability is fixed in versions [2.1.34.0 and later](#) when shipped on new devices for initial installation of the Cisco Wireless Location Appliance software.

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 WLA and changing the default password for the administrative root account to a strong password chosen by the user.

If the password has not previously been changed, the default username for the administrator login is "root" (without the quotes), and the default password is "password" (without the quotes). Both the username and password are case sensitive. After successfully logging in to the WLA as root, the default password may be changed by running the **passwd** command.

A reboot is not required for the new password to take effect, so network operations will not be disrupted.

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.

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.

Exploitation and Public Announcements

The Cisco PSIRT is aware of several instances in which Cisco Wireless Location Appliances have been compromised via the default root password.

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-20061012-wla.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 1.0	2006–October–12	Initial public release.
--------------	-----------------	-------------------------

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>.

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

Updated: Oct 12, 2006

Document ID: 71780
