

Cisco Security Advisory: A Default Username and Password in WLSE and HSE Devices

Document ID: 50400

Advisory ID: cisco-sa-20040407-username

<http://www.cisco.com/warp/public/707/cisco-sa-20040407-username.shtml>

Revision 1.4

Last Updated 2004 April 12 1700 UTC (GMT)

For Public Release 2004 April 07 1600 UTC (GMT)

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

[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

A default username/password pair is present in all releases of the Wireless LAN Solution Engine (WLSE) and Hosting Solution Engine (HSE) software. A user who logs in using this username has complete control of the device. This username cannot be disabled. There is no workaround.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040407-username.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

These products are vulnerable:

- The affected software releases for WLSE are 2.0, 2.0.2 and 2.5.
- The affected software releases for HSE are 1.7, 1.7.1, 1.7.2 and 1.7.3.

Products Confirmed Not Vulnerable

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

Details

A hardcoded username and password pair is present in all software releases for all models of WLSE and HSE devices.

This vulnerability is documented in the Cisco Bug Toolkit as Bug ID [CSCsa11583](#) ([registered](#) customers only) for the WLSE and [CSCsa11584](#) ([registered](#) customers only) for the HSE.

CiscoWorks WLSE provides centralized management for the Cisco Wireless LAN infrastructure. It unifies the other components in the solution and actively employs them to provide continual "Air/RF" monitoring, network security, and optimization. The CiscoWorks WLSE also assists network managers by automating and simplifying mass configuration deployment, fault monitoring and alerting.

Cisco Hosting Solution Engine is a hardware-based solution to monitor and activate a variety of e-business services in Cisco powered data centers. It provides fault and performance information about the Layer 2-3 hosting infrastructure and Layer 4-7 hosted services.

Impact

Any user who logs in using this username has complete control of the device. One can add new users or modify details of the existing users, and change the device's configuration. Here are some more concrete examples of possible actions:

- For WLSE this means that an adversary can hide the presence of a rogue Access Point or change the Radio Frequency plan, potentially causing system-wide outages. The first action may cause long term loss of information confidentiality and integrity. The second action can yield Denial-of-Service (DOS).
- For HSE this may lead up to illegal re-directing of a Web site with the ultimate loss of revenue.
- In both cases the device itself may be used as a launching platform for further attacks. Such attacks could be directed at your organization, or towards a third party.

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.

For WLSE, users need to install the WLSE-2.x-CSCsa11583-K9.zip patch. The patch can be downloaded from <http://www.cisco.com/cgi-bin/tablebuild.pl/wlan-sol-eng> ([registered](#) customers only) . Installation instructions are included in the accompanying README file, WLSE-2.x-CSCsa11583-K9.readmeV3.txt, in that same download directory. This patch is applicable to WLSE 1105 and 1130 software releases 2.0, 2.0.2 and 2.5.

For HSE, users need to install the HSE-1.7.x-CSCsa11584.zip patch. The patch can be downloaded from <http://www.cisco.com/cgi-bin/tablebuild.pl/1105-host-sol> ([registered](#) customers only) . Installation instructions are included in the accompanying README file, HSE-1.7.x-CSCsa11584.readme.txt, in that same download directory. This patch is applicable to HSE 1105 for versions 1.7, 1.7.1, 1.7.2, and 1.7.3.

Workarounds

There is no workaround.

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.

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 will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20040407-username.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
- bugtraq@securityfocus.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- firewalls@lists.gnac.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 1.4	2004-April-12	Fixed URL for Cisco.com Downloads under Obtaining Fixed Software section.
Revision 1.3	2004-April-08	Updated Software Versions and Fixes section.
Revision	2004-April-08	Updated to include WLSE 1105 in

1.2		Software Versions and Fixes section.
Revision 1.1	2004 April 07	Correction in the Obtaining Fixed Software section.
Revision 1.0	2004 April 07	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: Apr 12, 2004

Document ID: 50400
