

Cisco Security Advisory: Multiple Vulnerabilities in Cisco Wireless LAN Controllers

Advisory ID: [cisco-sa-20090727-wlc](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20090727-wlc.shtml>

Revision 1.1

Last Updated 2009 October 15 2000 UTC (GMT)

For Public Release 2009 July 27 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

Multiple vulnerabilities exist in the Cisco Wireless LAN Controller (WLC) platforms. This security advisory outlines the details of the following vulnerabilities:

- Malformed HTTP or HTTPS authentication response denial of service vulnerability
- SSH connections denial of service vulnerability
- Crafted HTTP or HTTPS request denial of service vulnerability
- Crafted HTTP or HTTPS request unauthorized configuration modification vulnerability

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at: <http://www.cisco.com/warp/public/707/cisco-sa-20090727-wlc.shtml>

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

☐ Affected Products

☐ Vulnerable Products

Cisco 1500 Series, 2000 Series, 2100 Series, 4400 Series, 4100 Series, 4200 Series, Wireless Services Modules (WiSM), WLC Modules for Integrated Services Routers, and Cisco Catalyst 3750G Integrated Wireless LAN Controllers are affected by one or more of the following vulnerabilities:

- The malformed HTTP or HTTPS authentication response denial of service vulnerability affects software versions 3.2 and later.
- The SSH connections denial of service vulnerability affects software versions 3.2 and later.
- The crafted HTTP or HTTPS request denial of service vulnerability affects software versions 4.1 and later.
- The crafted HTTP or HTTPS request unauthorized configuration modification vulnerability affects software versions 3.2 and later.

Determination of Software Versions

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

- In the web interface, choose the **Monitor** tab, click **Summary** in the left pane, and note the **Software Version** field.

Note: Customers who use a WLC Module in an Integrated Services Router (ISR) will need to issue the **service-module wlan-controller 1/0** session command prior to performing the next step on the command line. Customers who use a Cisco Catalyst 3750G Switch with an integrated WLC Module will need to issue the **session <Stack-Member-Number> processor 1** session command prior to performing the next step on the command line.

- From the command-line interface, type **show sysinfo** and note the **Product Version** field, as shown in the following example:

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.. Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 5.1.151.0
RTOS Version..... Linux-2.6.10_mv1401
Bootloader Version... 4.0.207.0
Build Type..... DATA + WPS
<output suppressed>
```

Use the **show wism module <module number> controller 1 status** command on a Cisco Catalyst 6500 Series/7600 Series Switch if you are using a WiSM. Note the software version as demonstrated in the following example, which shows version 5.1.151.0.

```
Router#show wism module 3 controller 1 status

WiSM Controller 1 in Slot 3
Operational Status of the Controller
: Oper-Up
Service VLAN
: 192
```

```
Service Port
: 10
Service Port Mac Address
: 0011.92ff.8742
Service IP Address
: 192.168.10.1
Management IP Address
: 192.168.1.123
Software Version
: 5.1.151.0
Port Channel Number
: 288
Allowed vlan list
: 30,40
Native VLAN ID
: 40
WCP Keep Alive Missed
: 0
```

☐ Products Confirmed Not Vulnerable

The Cisco Wireless Controller 5500 Series is not affected by these vulnerabilities.

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

☐ Details

Cisco Wireless LAN Controllers (WLCs) are responsible for system-wide wireless LAN functions, such as security policies, intrusion prevention, RF management, quality of service (QoS), and mobility.

These devices communicate with controller-based access points over any Layer 2 (Ethernet) or Layer 3 (IP) infrastructure using the Lightweight Access Point Protocol (LWAPP).

This security advisory describes multiple distinct vulnerabilities in the WLC family of devices.

- **Malformed HTTP or HTTPS authentication response denial of service vulnerability**
An attacker with access to the administrative web interface via HTTP or HTTPS may cause the device to reload by providing a malformed response to an authentication request.

Note: The vulnerability can be exploited only via the administrative web-based interface; Web Authentication features are not affected.

This vulnerability is documented in Cisco Bug ID [CSCsx03715](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2009-1164.

- **SSH connections denial of service vulnerability**
Affected devices may be susceptible to a memory leak when they handle SSH management connections. An attacker could use this behavior to cause an affected device to crash and reload.

Note: A three-way handshake is not required to exploit this vulnerability.

This vulnerability is documented in Cisco Bug ID [CSCsw40789](#) ([registered](#) customers only) and has been assigned CVE ID CVE-2009-1165.

- **Crafted HTTP or HTTPS request denial of service vulnerability**
An attacker with the ability to send a malicious HTTP request to an affected WLC could cause the device to crash and reload.

Note: The vulnerability can be exploited only via the administrative web-based interface; Web Authentication features are not affected.

This vulnerability is documented in Cisco Bug ID [CSCsy27708](#) ([registered](#) customers only) and has been assigned CVE ID CVE-2009-1166.

- **Crafted HTTP or HTTPS request unauthorized configuration modification vulnerability**

An unauthorized configuration modification vulnerability exists in all software versions prior to the first fixed release. A remote, unauthenticated attacker who can submit HTTP or HTTPS requests to the WLC directly could gain full control of the affected device.

Note: The vulnerability can be exploited only by submitting such a request to an IP address that is bound to an administrative interface or VLAN.

The vulnerability is documented by Cisco Bug ID [CSCsy44672](#) ([registered](#) customers only) and has been assigned CVE ID CVE-2009-1167.

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

▣ Vulnerability Scoring Details

Cisco has provided 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.

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

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

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>.

CSCsx03715 - Malformed HTTP or HTTPS authentication response denial of service vulnerability					
Calculate the environmental score of CSXsx03715					
CVSS Base Score - 7.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete

CVSS Temporal Score - **6.4**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

CSCsw40789 - SSH connections denial of service vulnerabilityCalculate the environmental score of [CSCsw40789](#)CVSS Base Score - **7.8**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete

CVSS Temporal Score - **6.4**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

CSCsy27708 - Crafted HTTP or HTTPS request denial of service vulnerabilityCalculate the environmental score of [CSCsy27708](#)CVSS Base Score - **7.8**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete

CVSS Temporal Score - 6.4

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

CSCsy44672 - Crafted HTTP or HTTPS request unauthorized configuration modification vulnerabilityCalculate the environmental score of [CSCsy44672](#)**CVSS Base Score - 10**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete

CVSS Temporal Score - 8.7

Exploitability	Remediation Level	Report Confidence
High	Official-Fix	Confirmed

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

Successful exploitation of the denial of service (DoS) vulnerabilities may cause the affected device to reload. Repeated exploitation could result in a sustained DoS condition.

An unauthenticated, remote attacker may be able to use the unauthorized configuration modification vulnerability to gain full control over the Wireless LAN Controller if the attacker is able to submit a crafted request directly to an administrative interface of the affected device.

[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.

Vulnerability/Bug ID	Affected Release	First Fixed Version	Recommended Release
Malformed HTTP or HTTPS authentication response denial of service vulnerability (CSCsx03715)	3.2	3.2.215.0	3.2.215.0
	4.1	Not Vulnerable	Not Vulnerable
	4.1M	Not Vulnerable	Not Vulnerable
	4.2	4.2.205.0	4.2.207.0
	4.2M	Not Vulnerable	Not Vulnerable
	5.0	Migrate to 5.2 or 6.0	5.2.193.0 or 6.0.182.0
	5.1	Migrate to 5.2 or 6.0	5.2.193.0 or 6.0.182.0
	5.2	5.2.178.0	5.2.193.0 or 6.0.182.0
	6.0	Not Vulnerable	Not Vulnerable
	3.2	3.2.215.0	3.2.215.0

SSH connections denial of service vulnerability (CSCsw40789)	4.1	Migrate to 4.2	4.2.205.0
	4.1M	Migrate to 5.2, 6.0, or 4.2M	5.2.193.0, 6.0.182.0 or 4.2.176.51 Mesh
	4.2	4.2.205.0	4.2.207.0
	4.2M	Not Vulnerable	Not Vulnerable
	5.0	Migrate to 5.2 or 6.0	5.2.193.0 or 6.0.182.0
	5.1	5.1.163.0	5.2.193.0 or 6.0.182.0
	5.2	5.2.178.0	5.2.193.0 or 6.0.182.0
	6.0	Not Vulnerable	Not Vulnerable
	3.2	Not Vulnerable	Not Vulnerable
	4.1	Migrate to 4.2	4.2.205.0
	4.1 M	Migrate to 5.2, 6.0, or 4.2M	5.2.193.0, 6.0.182.0 or 4.2.176.51 Mesh
	4.2	4.2.205.0	4.2.207.0

Crafted HTTP request may cause the WLC to crash (CSCsy27708)	4.2M	Not Vulnerable	Not Vulnerable
	5.0	Migrate to 5.2 or 6.0	5.2.193.0 or 6.0.182.0
	5.1	Migrate to 5.2 or 6.0	5.2.193.0 or 6.0.182.0
	5.2	5.2.191.0	5.2.193.0 or 6.0.182.0
	6.0	Not Vulnerable	Not Vulnerable
Crafted HTTP or HTTPS request unauthorized configuration modification vulnerability (CSCsy44672)	3.2	3.2.215.0	3.2.215.0
	4.1	Migrate to 4.2	4.2.205.0
	4.1M	Migrate to 5.2, 6.0, or 4.2M	5.2.193.0, 6.0.182.0 or 4.2.176.51 Mesh
	4.2	4.2.205.0	4.2.207.0
	4.2M	Not Vulnerable	Not Vulnerable
	5.0	Migrate to 5.2 or 6.0	5.2.193.0, 6.0.182.0
	5.1	Migrate to 5.2 or 6.0	5.2.193.0 or 6.0.182.0
	5.2	5.2.191.0	5.2.193.0 or

			6.0.182.0
	6.0	Not Vulnerable	Not Vulnerable

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

Workarounds

The SSH connections denial of service vulnerability identified by Cisco Bug ID CSCsw40789 may be remediated by disabling SSH on the affected device. This workaround requires subsequent management of the device to be performed using the HTTP/HTTPS web management interface or the serial console of the device.

Additional mitigations that can be deployed on Cisco devices in the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory, which is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-amb-20090727-wlc.shtml>

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

Obtaining Fixed Software

Cisco has released free software updates that address these vulnerabilities. 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/en/US/docs/general/warranty/English/EU1KEN_.html, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact 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 agreements 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 do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html for additional TAC contact information, including 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 at the time of release.

The DoS vulnerability documented by CSCsw40789 was discovered during the resolution of customer support cases.

The unauthorized configuration modification vulnerability documented by CSCsy44672 was found during internal testing.

The DoS vulnerability documented by CSCsx03715 was discovered by Christoph Bott of SySS GmbH.

The DoS vulnerability documented by CSCsy27708 was discovered by IBM Research.

[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-20090727-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-bulletins@lists.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	2009-October-15	Added information about WLC Release 3.2 in the Vulnerable Products section and Software Versions and Fixes table.
Revision 1.0	2009-July-27	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](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)