

Cisco Security Advisory: Multiple Vulnerabilities in Cisco Wireless LAN Controllers

Advisory ID: cisco-sa-20090204-wlc

<http://www.cisco.com/warp/public/707/cisco-sa-20090204-wlc.shtml>

Revision 1.3

Last Updated 2009 October 15 2000 UTC (GMT)

For Public Release 2009 February 04 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 Controllers (WLCs), Cisco Catalyst 6500 Wireless Services Modules (WiSMs), and Cisco Catalyst 3750 Integrated Wireless LAN Controllers. This security advisory outlines details of the following vulnerabilities:

- Denial of Service Vulnerabilities (total of three)
- Privilege Escalation Vulnerability

These vulnerabilities are independent of each other.

Cisco has released free software updates that address these vulnerabilities.

There are no workarounds available for these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090204-wlc.shtml>.

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

☐ Affected Products

☐ Vulnerable Products

The following products and software versions are affected for each vulnerability.

Denial of Service Vulnerabilities

Two denial of service (DoS) vulnerabilities affect software versions 4.1 and later. All Cisco Wireless LAN Controller (WLC) platforms are affected.

A third DoS vulnerability affects software versions 4.1 and later. The following platforms are affected by this vulnerability:

- Cisco 4400 Series Wireless LAN Controllers
- Cisco Catalyst 6500 Series/7600 Series Wireless Services Module (WiSM)
- Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers

Note: The Cisco Wireless LAN Controller Modules supported on Cisco 2800 and 3800 series Integrated Services Routers are not vulnerable. The Cisco 2000 and 2100 Series Wireless LAN Controllers are also not affected by this vulnerability.

Privilege Escalation Vulnerability

Only WLC software version 4.2.173.0 is affected by this vulnerability.

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**.
- From the command-line interface, type **show sysinfo** and note the **Product Version**, 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_mvl401
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 using a WiSM, and note the **Software Version**, as demonstrated in the following

example:

```
Router#show wism mod 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

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

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

☐ Details

Cisco Wireless LAN Controllers (WLCs), Cisco Catalyst 6500 Wireless Services Modules (WiSMs), and Cisco Catalyst 3750 Integrated Wireless LAN Controllers 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 WLCs, WiSMs, and the Cisco Catalyst 3750 Integrated WLCs. These vulnerabilities are independent of each other.

Denial of Service Vulnerabilities

These vulnerabilities are documented in the following Cisco Bug ID and have been assigned the following Common Vulnerabilities and Exposures (CVE) identifiers:

- [CSCsq44516](#) ([registered](#) customers only) - CVE-2009-0058
Web authentication is a Layer 3 security feature that causes the controller to drop IP traffic (except DHCP and DNS related packets) from a particular client until that client has correctly supplied a valid username and password. An attacker may use a vulnerability scanner to cause the device to stop servicing web authentication or cause a reload of the device. The following error messages may appear on the console during an active attack:

```
SshPmStMain/pm_st_main.c:1954/
ssh_pm_st_main_batch_addition_result:
Failed to add rule to the engine:
restoring old state
SshEnginePmApiPm/engine_pm_api_pm.c:1896/
```

```
ssh_pme_enable_policy_lookup:  
Could not allocate message
```

Note: The affected device must have Webauth configured to be vulnerable. Devices not configured for Webauth are not vulnerable.

- [CSCsm82364](#) ([registered](#) customers only) - CVE-2009-0059

An attacker may cause a device reload when sending a malformed post to the web authentication "login.html" page. The following error messages may appear on the WLC console during this attack:

```
Cisco Crash Handler  
Signal generated during a signal 11,  
count 193  
Memory 0x14ef1e44 has been freed!
```

Note: A crash file is not generated during this attack.

Note: The affected device must have Webauth configured to be vulnerable. Devices not configured for Webauth are not vulnerable.

- [CSCso60979](#) ([registered](#) customers only) - CVE-2009-0061

Affected Cisco WLC, WiSM and Catalyst 3750 Wireless LAN Controller models are vulnerable to a DoS condition that is triggered by the receipt of certain IP packets. Upon receiving these IP packets, the affected device may become unresponsive and require a reboot to recover.

Note: This vulnerability affects software versions 4.1 and later in the Cisco 4400 series WLCs, Cisco Catalyst 6500 WiSM, and the Cisco Catalyst 3750 Integrated Wireless LAN Controllers. Cisco 4100, 2100, and 2000 series WLCs are not affected by this vulnerability.

Note: Customers requiring FIPS compliance with Release 4.1.185.10 are not at risk to the vulnerabilities listed in this advisory:

[CSCsq44516](#) and [CSCsm82364](#)—Cisco WLAN Controller FIPS compliance prohibits Webauth functionality from being enabled. Devices not configured for Webauth are not effected by these vulnerabilities.

[CSCso60979](#)—Release 4.1.185.10 is not affected by this vulnerability.

Privilege Escalation Vulnerability

A privilege escalation vulnerability exists only in WLC software version 4.2.173.0, and could allow a restricted user (i.e., Lobby Admin) to gain full administrative rights on the affected system.

Note: Wireless network users are not affected by this vulnerability.

This vulnerability is documented in Cisco Bug ID [CSCsv62283](#) ([registered](#) customers only) and has been assigned the Common Vulnerabilities and Exposures (CVE) identifier CVE-2009-0062.

[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>.

| | | | | | |
|---|-------------------|-------------------|------------------------|-------------------|---------------------|
| CSCsq44516 - Certain packets may cause WebAuth services to hang or reload the device | | | | | |
| Calculate the environmental score of CSCsq44516 | | | | | |
| CVSS Base Score - 6.1 | | | | | |
| Access Vector | Access Complexity | Authentication | Confidentiality Impact | Integrity Impact | Availability Impact |
| Adjacent Network | Low | None | None | None | Complete |
| CVSS Temporal Score - 5 | | | | | |
| Exploitability | | Remediation Level | | Report Confidence | |
| Functional | | Official-Fix | | Confirmed | |

| | | | | | |
|--|-------------------|----------------|------------------------|------------------|---------------------|
| CSCsm82364 - Crash handling invalid post for webauth | | | | | |
| Calculate the environmental score of CSCsm82364 | | | | | |
| CVSS Base Score - 6.1 | | | | | |
| Access Vector | Access Complexity | Authentication | Confidentiality Impact | Integrity Impact | Availability Impact |
| | | | | | |

| | | | | | |
|--------------------------------|-----|-------------------|------|-------------------|----------|
| Adjacent Network | Low | None | None | None | Complete |
| CVSS Temporal Score - 5 | | | | | |
| Exploitability | | Remediation Level | | Report Confidence | |
| Functional | | Official-Fix | | Confirmed | |

CSCso60979 - WLC TSEC driver may hang or crash the device

Calculate the environmental score of [CSCso60979](#)

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 | |

CSCsv62283 - Local Management Users may obtain full admin rights

Calculate the environmental score of [CSCsv62283](#)

CVSS Base Score - 9

| | | | | | |
|---------------|-------------------|----------------|------------------------|------------------|---------------------|
| Access Vector | Access Complexity | Authentication | Confidentiality Impact | Integrity Impact | Availability Impact |
| | | | | | |

| | | | | | |
|----------------------------------|-----|-------------------|----------|-------------------|----------|
| Network | Low | Single | Complete | Complete | Complete |
| CVSS Temporal Score - 7.8 | | | | | |
| Exploitability | | Remediation Level | | Report Confidence | |
| High | | Official-Fix | | Confirmed | |

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

▣ Impact

Successful exploitation of the denial of service vulnerabilities may cause the affected device to hang or reload. Repeated exploitation could result in a sustained DoS condition. The privilege escalation vulnerability may allow an authenticated user to obtain full administrative rights on the 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.

| Vulnerability/ Bug ID | Affected Release | First Fixed Version | Recommended Release |
|--------------------------|------------------|------------------------|------------------------------|
| CSCsq44516 | 3.2 | 3.2.215.0 | 3.2.215.0 |
| | 4.1 | Migrate to 4.2 | 4.2.176.0 |
| | 4.1M | Migrate to 5.2 or 4.2M | 5.2.178.0 or 4.2M (see note) |
| | 4.2 | 4.2.173.0 | 4.2.176.0 |

| | | | |
|------------|-------|---------------------------|---------------------------------|
| | 5.0 | Migrate to 5.2 | 5.2.178.0 |
| | 5.1 | 5.1.163.0 | 5.1.163.0 |
| | 5.2 | Not vulnerable | Not Vulnerable |
| CSCsm82364 | 3.2 | 3.2.215.0 | 3.2.215.0 |
| | 4.1 | Migrate to 4.2 | 4.2.176.0 |
| | 4.1M | Migrate to 5.2 or 4.2M | 5.2.178.0 or 4.2M (see note) |
| | 4.2 | 4.2.112.0 | 4.2.176.0 |
| | 5.0 | Not vulnerable | Not vulnerable |
| | 5.1 | Not vulnerable | Not vulnerable |
| | 5.2 | Not vulnerable | Not vulnerable |
| CSCso60979 | 3.2 | 3.2.215.0 | 3.2.215.0 |
| | 4.1 | 4.1.185.10 | 4.2.176.0 |
| | 4.1 M | Migrate to 5.2 or 4.2M | 5.2.178.0 or 4.2M (see note) |
| | 4.2 | 4.2.117.0 | 4.2.176.0 |
| | 5.0 | Migrate to 5.2 | 5.2.178.0 |
| | 5.1 | Not vulnerable | Not vulnerable |

| | | | |
|------------|------|----------------|----------------|
| | 5.2 | Not vulnerable | Not vulnerable |
| CSCsv62283 | 3.2 | Not vulnerable | Not vulnerable |
| | 4.1 | Not vulnerable | Not vulnerable |
| | 4.1M | Not vulnerable | Not vulnerable |
| | 4.2 | 4.2.174.0 | 4.2.176.0 |
| | 5.0 | Not Vulnerable | Not Vulnerable |
| | 5.1 | Not Vulnerable | Not vulnerable |
| | 5.2 | Not Vulnerable | Not vulnerable |

Note: Customers running 4.1M (Mesh) should migrate as follows:

- If using AP1505/AP1510, migrate to 4.2M (targeted for 2HCY09).
- If using AP1520 or indoor mesh, migrate to 5.2.178.0.

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

Workarounds

There are no workarounds for any of these vulnerabilities.

[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. These vulnerabilities were found during internal testing and during the resolution 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-20090204-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 1.3 | 2009-October-15 | Added information about WLC release 3.2 in the Software Versions and Fixes table. |
| Revision 1.2 | 2009-March-11 | Added 4.1M release and revised information for 5.0 and 5.2 releases in the Software Versions and Fixes table. |
| Revision 1.1 | 2009-February-11 | Update with additional FIPS information. |
| Revision 1.0 | 2009-February- | Initial public release. |

04

[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.](#)