

# Cisco Security Advisory: Wireless ARP Storm Vulnerabilities

Document ID: 97823

Advisory ID: cisco-sa-20070724-arp

<http://www.cisco.com/warp/public/707/cisco-sa-20070724-arp.shtml>

## Revision 1.1

Last Updated 2007 July 31 1436 UTC (GMT)

For Public Release 2007 July 24 1600 UTC (GMT)

---

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

---

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of this Notice: INTERIM](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

---

## Summary

Cisco Wireless LAN Controllers (WLC) contain multiple vulnerabilities in the handling of Address Resolution Protocol (ARP) packets that could result in a denial of service (DoS) in certain environments.

Cisco is notifying customers and partners and has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070724-arp.shtml>.

## Affected Products

Unless otherwise specified, the vulnerabilities addressed in this document affect versions 4.1, 4.0, 3.2, and prior versions of the Wireless LAN Controller software. To identify the earliest software releases that include fixes for these vulnerabilities, please consult the Software Versions and Fixes section of this advisory.

To determine the version of WLC system software running on a particular device, one of the following methods may be used:

- In the web interface, choose the **Monitor** tab, click **Summary** in the left-hand pane, and note the "Software Version."
- From the command-line interface, type **show sysinfo** and note the "Product Version."

## Vulnerable Products

Vulnerable versions of software may be running on any of the following hardware platforms:

- Cisco 4100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco Aireospace 4000 Series Wireless LAN Controller
- Cisco Catalyst 6500 Series Wireless Services Module (WiSM)
- Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers

## Products Confirmed Not Vulnerable

The following hardware platforms are not affected by these vulnerabilities:

- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco Aireospace 3500 Series WLAN Controller
- Cisco 526 Wireless Express Mobility Controller
- Cisco Wireless LAN Controller Module  
(NM-AIR-WLC6-K9,NME-AIR-WLC8-K9,NME-AIR-WLC12-K9)
- Standalone Access Points such as the 1100 Series, 1200 Series and AP340/350
- Cisco 3800 Series Integrated Services Routers
- Cisco 2800 Series Integrated Services Routers
- Cisco 1800 Series Integrated Services Routers
- Cisco 800 Series Routers

## Details

Cisco Wireless LAN Controllers provide real-time communication between lightweight access points and other Wireless LAN controllers for centralized system wide WLAN configuration and management functions.

The Address Resolution Protocol, or ARP, provides a mapping between a device's IP address and its hardware address on the local network.

The WLC contains vulnerabilities in the processing of unicast ARP traffic where a unicast ARP request may be flooded on the LAN links between Wireless LAN Controllers in a mobility group.

[RFC4436](#) defines a method for IP Version 4 hosts to detect if they have re-attached to a previously attached network. In such cases, it may be unnecessary to request a new DHCP address lease if the current lease is still active. To determine reattachment, the host may send a unicast ARP request to the address of the default gateway that it had previously used.

A vulnerable WLC may mishandle unicast ARP requests from a wireless client leading to an ARP storm. In order for the vulnerability to be exposed, two WLCs attached to the same set of Layer-2 VLANs must each have a context for the wireless client. This can occur after a Layer-3 (cross-subnet) roam or when guest WLAN (auto-anchor) is in use.

If the client sends a unicast ARP request with a destination MAC address that has not been learned by the Layer-2 infrastructure, that request will be flooded to all ports in the Layer-2 domain after egressing the

WLC. This allows the second WLC to reprocess the ARP request and incorrectly reforward this packet back into the network. This vulnerability is documented as [CSCsj69233](#) ([registered](#) customers only) .

If the arpunicast feature has been enabled on the WLC, the WLC will re-forward broadcast ARP packets targeting the IP address of a known client context. This creates an ARP storm if more than one WLC is installed on the corresponding VLAN. This vulnerability is documented as [CSCsj50374](#) ([registered](#) customers only) and only affects version 4.1 of the WLC software (versions 4.0, 3.2, or previous versions are not affected).

In a Layer-3 (L3) roaming scenario, a wireless client moves from one controller to another where the wireless LAN interfaces configured on different controllers are on different IP subnets. In this scenario, a unicast ARP may not tunneled back to the anchor controller, but may instead be sent by the foreign controller out to a local VLAN. This vulnerability is documented as [CSCsj70841](#) ([registered](#) customers only) .

Note: In versions of software prior to 4.1, a unicast ARP request from a wireless client that performed a Layer-3 roam was dropped at the Foreign WLC. This behavior has been corrected as part of [CSCsj70841](#) ([registered](#) customers only) .

## 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 1.0.

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.

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

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>.

CSCsj69233 ( <a href="#">registered</a> customers only)						
CVSS Base Score – 3.3						
Access Vector	Access	Authentication	Confidentiality	Integrity	Availability	Impact
Remote	Complexity Low	Not Required	Impact None	Impact None	Impact Complete	Bias Normal
CVSS Temporal Score – 2.7						
Exploitability	Remediation Level			Report Confidence		
Functional	Official Fix			Confirmed		

CSCsj50374 ( <a href="#">registered</a> customers only)						
CVSS Base Score – 3.3						
Access Vector	Access	Authentication	Confidentiality	Integrity	Availability	Impact
Remote	Complexity Low	Not Required	Impact None	Impact None	Impact Complete	Bias Normal
CVSS Temporal Score – 2.7						
Exploitability	Remediation Level			Report Confidence		
Functional	Official Fix			Confirmed		

CSCsj70841 ( <a href="#">registered</a> customers only)						
CVSS Base Score – 4.7						
Access Vector	Access	Authentication	Confidentiality	Integrity	Availability	Impact
Remote	Complexity Low	Not Required	Impact None	Impact Partial	Impact Partial	Bias Normal
CVSS Temporal Score – 3.9						
Exploitability	Remediation Level			Report Confidence		
Functional	Official Fix			Confirmed		

## Impact

Successful exploitation of these vulnerabilities may result in a DoS condition.

## 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.

Major Release	Availability of Fixed Releases
3.2	3.2.195.13
4.0	4.0.219.0
4.1	4.1.181.0

## Workarounds

For enhanced security, Cisco recommends that operators require all clients to obtain their IP addresses from a DHCP server. To enforce this requirement, all WLANs can be configured with a **DHCP Required** setting, which disallows client static IP addresses. If **DHCP Required** is selected, clients must obtain an IP address via DHCP. Any client with a static IP address will not be allowed on the network. The controller monitors DHCP traffic because it acts as a DHCP proxy for the clients.

This workaround is generally effective for wireless clients employing the mechanisms defined in [RFC4436](#) when joining a network. It is not effective against deliberate attempts to craft packets that create an ARP storm.

Customers experiencing exploitation from the vulnerability associated with [CSCsj50374](#) ([registered](#) customers only) may configure the WLC to disable arpunicast processing via the CLI:

```
config network arpunicast disable
```

This section provides both GUI and CLI instructions for configuring your WLAN to use a DHCP server.

## Using the GUI to Configure DHCP

1. In the web user interface, navigate to the WLANs page.
2. Locate the WLAN you wish to configure for a DHCP server, and click the associated Edit link to display the WLANs > Edit page.
3. Under General Policies, check the **DHCP Relay/DHCP Server IP Addr** check box to verify whether you have a valid DHCP server assigned to the WLAN. If you do not have a DHCP server assigned to the WLAN, continue with Step 4. Otherwise, continue with Step 9.
4. Under General Policies, uncheck the **Admin Status** check box.
5. Click **Apply** to disable the WLAN.
6. In the DHCP Relay/DHCP Server IP Addr edit box, enter a valid DHCP server IP address for this WLAN.
7. Under General Policies, check the **Admin Status** check box.
8. Click **Apply** to assign the DHCP server to the WLAN and to enable the WLAN. You are then returned to the WLANs page.
9. In the upper-right corner of the WLANs page, click **Ping** and enter the DHCP server IP address to verify that the WLAN can communicate with the DHCP server.

## Using the CLI to Configure DHCP

1. In the CLI, enter **show wlan** to verify whether you have a valid DHCP server assigned to the WLAN. If you do not have a DHCP server assigned to the WLAN, continue with Step 2. Otherwise, continue with Step 4.
2. If necessary, use the following commands:

```
config wlan disable <wlan-id>  
config wlan dhcp_server <wlan-id> <dhcp-server-ip-address>  
config wlan enable <wlan-id>
```

In these commands, wlan-id = 1 through 16, and dhcp-server-ip-address = DHCP server IP address.

3. Enter **show wlan** to verify that you have a DHCP server assigned to the WLAN.
4. Enter **ping dhcp-ip-address** to verify that the WLAN can communicate with the DHCP server.

## Obtaining Fixed Software

Cisco will make free software available to address these vulnerabilities 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](mailto: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 malicious use of the vulnerabilities described in this advisory.

These vulnerabilities were reported to Cisco by customers.

## Status of this Notice: INTERIM

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. CISCO EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE.

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-20070724-arp.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	2007-July-31	Updated fixed software version information
Revision 1.0	2007-July-24	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](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: Jul 31, 2007

Document ID: 97823

---