

Cisco Security Advisory: Access Point Memory Exhaustion from ARP Attacks

Document ID: 68715

Advisory ID: cisco-sa-20060112-wireless

<http://www.cisco.com/warp/public/707/cisco-sa-20060112-wireless.shtml>

Revision 1.0

For Public Release 2006 January 12 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 vulnerability exists in Cisco Aironet Wireless Access Points (AP) running IOS which may allow a malicious user to send a crafted attack via IP address Resolution Protocol (ARP) to the Access point which will cause the device to stop passing traffic and/or drop user connections.

Repeated exploitation of this vulnerability will create a sustained DoS (denial of service).

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20060112-wireless.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

This security advisory applies to all Cisco Aironet Wireless Access Points that run Cisco IOS Software. The affected device types include:

- Cisco Aironet 1400 Series Wireless Bridges
- Cisco Aironet 1300 Series Access Points
- Cisco Aironet 1240AG Series Access Points
- Cisco Aironet 1230AG Series Access Points
- Cisco Aironet 1200 Series Access Points
- Cisco Aironet 1130AG Series Access Points
- Cisco Aironet 1100 Series Access Points
- Cisco Aironet 350 Series Access Points running IOS

Products Confirmed Not Vulnerable

Cisco Wireless devices running a VxWorks based image (Version 12.05 and earlier)

No other Cisco products are currently known to be affected by this vulnerability.

Details

The Address Resolution Protocol (ARP) is used to dynamically map physical hardware addresses to an IP address. Network devices and workstations maintain internal tables in which these mappings are stored for some period of time.

An attacker, who has successfully associated with a Cisco IOS Wireless Access Point, may be able to spoof ARP messages to the management interface on the Access Point. The attacker could add entries to the ARP table on the device until physical memory has been completely exhausted. This will leave the device in a state where it is unable to pass traffic until the device has been reloaded by cycling the power.

After upgrading the Access Point (see Software Versions and Fixes), add the command L2-FILTER BLOCK-ARP to each radio interface.

EXAMPLE:

```
!  
!  
interface Dot11Radio0  
  l2-filter block-arp  
!  
!
```

This vulnerability is documented in the Cisco Bug Toolkit as Bug ID [CSCsc16644](#) ([registered](#) customers only)

Impact

Successful exploitation of this vulnerability may result in a denial of service (DoS) impacting the availability of the Wireless Access Point. Management and packet forwarding services will be unavailable.

Software Versions and Fixes

This issue is fixed in IOS version 12.3-7-JA2 which is available for download at <http://www.cisco.com/kobayashi/sw-center/sw-wireless.shtml>.

It is important to note that in addition to the software upgrade, a configuration change is also necessary to resolve this vulnerability. Please see the Details section for information on this configuration change.

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 workaround for this issue is to use Virtual LANs (VLANs) to isolate wireless clients from the Access Point (AP) management interface. A wireless VLAN infrastructure can be deployed that places AP management interfaces in one VLAN and places wireless clients into different VLANs based on SSID. No wireless clients should be allowed on the same VLAN as the management interface of the AP. There are several design considerations that must be accounted for when deploying VLANs on the wireless network. For a discussion of the prerequisites, design considerations, and wireless and wired hardware configuration examples refer to:

Using VLANs with Cisco Aironet Wireless Equipment

http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_example09186a00801d0815.shtml

Additional information is available at:

Configuring VLANs

http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_guide_chapter09186a0080341d34.

In this example an existing AP is reconfigured to use VLANs. The AP is configured in VLAN 10 (the native VLAN) and wireless clients are configured in VLANS 20 and 30.

Creating VLANs will disable existing SSIDs. So for this example, the existing SSID was deleted, the VLANs were created, Encryption Mode and Keys were then set for each VLAN, and SSIDs were created for each VLAN.

```
!
! Set encryption ciphers and broadcast key rotation
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers tkip
!
encryption vlan 10 mode ciphers tkip
! Encryption ciphers are set under the physical radio interface
!
encryption vlan 20 mode ciphers tkip
!
encryption vlan 30 mode ciphers tkip
!
broadcast-key change 43000
!
broadcast-key vlan 10 change 43000
! Broadcast key rotation is set under the physical radio interface
!
broadcast-key vlan 20 change 43000
!
broadcast-key vlan 30 change 43000
!
```

```

!
!
! Set the SSID's and their vlans and authentication method
!
ssid ap-devices-only
! each SSID must have a vlan and authentication settings
  vlan 10
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa
!
ssid red20
  vlan 20
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa
!
ssid red30
  vlan 30
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa

!-----
! Consider not configuring an SSID for the native VLAN
! which in this example is VLAN 10. Not configuring an
! SSID for the native VLAN will prevent all wireless
! clients from establishing management connections to
! the AP
!-----

!

interface Dot11Radio0.10
  encapsulation dot1Q 10 native
! AP's are placed in this VLAN
  no ip proxy-arp
  no ip route-cache
  no cdp enable
  bridge-group 1
  bridge-group 1 spanning-disabled
! If the virtual interfaces are configured via the HTTP GUI
! the bridge-group settings will be configured automatically
!
interface Dot11Radio0.20
  encapsulation dot1Q 20
! Clients are placed in this VLAN
  no ip route-cache
  no cdp enable
  bridge-group 20
  bridge-group 20 subscriber-loop-control
  bridge-group 20 block-unknown-source
  no bridge-group 20 source-learning
  no bridge-group 20 unicast-flooding
  bridge-group 20 spanning-disabled
!
interface Dot11Radio0.30
  encapsulation dot1Q 30
! Clients are placed in this VLAN
  no ip route-cache
  no cdp enable
  bridge-group 30
  bridge-group 30 subscriber-loop-control
  bridge-group 30 block-unknown-source
  no bridge-group 30 source-learning

```

```

no bridge-group 30 unicast-flooding
bridge-group 30 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
no cdp enable
!
!
! Set the Wired virtual interfaces
!
interface FastEthernet0.10
encapsulation dot1Q 10 native
no ip proxy-arp
no ip route-cache
no cdp enable
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
! If the virtual interfaces are configured via the HTTP GUI
! the bridge-group settings will be configured automatically
!
interface FastEthernet0.20
encapsulation dot1Q 20
no ip route-cache
no cdp enable
bridge-group 20
no bridge-group 20 source-learning
bridge-group 20 spanning-disabled
!
interface FastEthernet0.30
encapsulation dot1Q 30
no ip route-cache
no cdp enable
bridge-group 30
no bridge-group 30 source-learning
bridge-group 30 spanning-disabled
!
!
! The AP's BVI1 IP address must be from the native VLAN's subnet
!
interface BVI1
ip address 192.168.1.40 255.255.255.0
no ip route-cache

```

Wireless Network Security Best Practices

In addition to the above workarounds and example, Cisco recommends deploying Wireless network security best practices which are discussed in the references below:

SAFE: Wireless LAN Security in Depth – version 2

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8b3..

Wireless LAN Security Solution for Large Enterprise

http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns386/networking_solutions_package.html

Cisco Wireless LAN Security Overview

Mitigation

The risk of this issue can be mitigated by requiring all wireless clients to authenticate with an EAP based authentication protocol such as EAP-FAST, PEAP, or EAP-TLS. However authenticated users could still exploit this vulnerability as the mitigation cannot completely eliminate the vulnerability.

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 malicious use of the vulnerability described in this advisory.

This issue was reported to us by Eric Smith at Bucknell University.

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-20060112-wireless.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	12-January-2006	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: Jan 12, 2006

Document ID: 68715
