

[NEWS] ARP Attacks Access Point Memory Exhaustion

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00045.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 15 Jan 2006 19:02:16 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

ARP Attacks Access Point Memory Exhaustion

SUMMARY

A vulnerability exists in Cisco Aironet Wireless Access Points (AP) running IOS that 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).

DETAILS

Vulnerable Systems:

- * 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

[NEWS] ARP Attacks Access Point Memory Exhaustion

Immune Systems:

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

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.

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.

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.htm

[NEWS] ARP Attacks Access Point Memory Exhaustion

Using VLANs with Cisco Aironet Wireless Equipment

Additional information is available at:

Configuring VLANs

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

Configuring VLANs

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
```

[NEWS] ARP Attacks Access Point Memory Exhaustion

```
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
```

[NEWS] ARP Attacks Access Point Memory Exhaustion

```
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 BV11 IP address must be from the native VLAN's subnet
!
interface BV11
ip address 192.168.1.40 255.255.255.0
no ip route-cache
```

[NEWS] ARP Attacks Access Point Memory Exhaustion

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_paper09186a008009c8b2>

SAFE: Wireless LAN Security in Depth – version 2

Wireless LAN Security Solution for Large Enterprise

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

Wireless LAN Security Solution for Large Enterprise

<http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a00801f7d0b.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.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:psirt@xxxxxxxx>> Cisco Systems Product Security Incident Response Team.

The original article can be found at:

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

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

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

[NEWS] ARP Attacks Access Point Memory Exhaustion

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- Prev by Date: [*\[NT\] Cisco Security Agent Vulnerable to Crafted IP Attack*](#)
- Next by Date: [*\[NEWS\] Apple QuickTime STSD Atom Heap Overflow*](#)
- Previous by thread: [*\[NT\] Cisco Security Agent Vulnerable to Crafted IP Attack*](#)
- Next by thread: [*\[NEWS\] Apple QuickTime STSD Atom Heap Overflow*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)