

# [NEWS] Cisco IOS DHCP Blocked Interface DoS

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0032.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 11/11/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 11 Nov 2004 18:33:31 +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>

-----

Cisco IOS DHCP Blocked Interface DoS

---

## SUMMARY

Cisco IOS devices running several branches of Cisco IOS that have Dynamic Host Configuration Protocol (DHCP) server or relay agent enabled, even if not configured, are vulnerable to a denial of service where the input queue becomes blocked when receiving specifically crafted DHCP packets.

## DETAILS

### Vulnerable Versions:

\* Any Cisco device running IOS versions 12.2(18)EW, 12.2(18)EWA, 12.2(14)SZ, 12.2(18)S, 12.2(18)SE, 12.2(18)SV, 12.2(18)SW

### Vulnerable Systems:

- \* Cisco 7200, 7300, 7500 platforms
- \* Cisco 2650, 2651, 2650XM, 2651XM Multiservice platform
- \* Cisco ONS15530, ONS15540
- \* Cisco Catalyst 4000, Sup2plus, Sup3, Sup4 and Sup5 modules
- \* Cisco Catalyst 4500, Sup2Plus TS
- \* Cisco Catalyst 4948, 2970, 3560, and 3750
- \* Cisco Catalyst 6000, Sup2/MSFC2 and Sup720/MSFC3
- \* Cisco 7600 Sup2/MSFC2 and Sup720/MSFC3

## Securiteam: [NEWS] Cisco IOS DHCP Blocked Interface DoS

### Immune Systems:

- \* 700 series dialup routers (750, 760, and 770 series) are not affected.
- \* WAN switching products such as the IGX, BPX and MGX lines are not affected.
- \* No host-based software is affected.
- \* The Cisco PIX Firewall is not affected
- \* The Cisco LocalDirector is not affected.
- \* The Cisco Content Engine and ACNS is not affected.
- \* The Catalyst 2901/2902, 2948G, 2980G, 4000, 5000, and 6000 switches running CatOS.
- \* Cisco Network Registrar is not affected.
- \* Cisco VPN 3000 series is not affected
- \* Cisco IOS-XR platform is not affected.
- \* Cisco MDS 9000 family is not affected.

Note: Any other Cisco device running IOS of a version not listed above in the affected versions section or Cisco products running an affected version with the option 'no service dhcp'.

DHCP services allow devices to request and receive basic host configuration information from the DHCP server via the network. Cisco routers can be configured to both provide dynamic host configuration information (termed DHCP server function), and forward DHCP and BootP packets across separate broadcast domains (termed DHCP relay agent function). Cisco routers are configured to process and accept DHCP packets by default, therefore the command "service dhcp" does not appear in the running configuration display, and only the command for the disabled feature, no service dhcp, will appear in the running configuration display when the feature is disabled.

The vulnerability is present, regardless if the DHCP server or relay agent configurations are present on an affected product. The only required configuration for this vulnerability in affected versions is the lack of the no service dhcp command. Certain crafted DHCP packets may be undeliverable, but will remain in the queue instead of being dropped. If a number of packets are sent that equal the size of the input queue, no more traffic will be accepted on that interface.

On a blocked Ethernet interface, Address Resolution Protocol (ARP) times out after a default time of four hours, and no inbound or outbound traffic can be processed, including both IP and non-IP traffic such as IPX. The device must be rebooted to clear the input queue on the interface, and will not reload without user intervention.

The attack may be repeated on all interfaces, causing the router to be remotely inaccessible, excluding the console port where DHCP packets are not processed by default and which can be used for out-of-band management and configured for remote access. Workarounds are available, and are documented in the Workarounds section below. Other types of interfaces, including but not limited to ATM, Serial and POS interfaces, are affected, but ARP is not a factor.

## Securiteam: [NEWS] Cisco IOS DHCP Blocked Interface DoS

To identify a blocked input interface, use the show interfaces command and look for the Input Queue line. The size of the input queue may keep increasing. If the current size (in this case, 76) is larger than the maximum size (75), the input queue is blocked. Example:

```
Router#show interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is 0050.500e.f1e0 (bia 0050.500e.f1e0)
  Internet address is 172.16.1.9/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load
1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:41, output 00:00:07, output hang never
  Last clearing of "show interface" counters 00:07:18
  Input queue: 76/75/1091/0 (size/max/drops/flushes); Total output
drops: 0
```

Note: The 76/75 queue count means the queue is blocked.

### Impact

A device receiving these specially crafted DHCP packets will force the inbound interface to stop processing traffic. The device may stop processing packets destined to the router, including routing protocol packets and ARP packets. No alarms will be triggered, nor will the router reload to correct itself. This vulnerability may be exercised repeatedly resulting in loss of availability until a workaround has been applied or the device has been upgraded to a fixed version of code.

The effects of this vulnerability can be monitored by the same methods outlined in the white paper entitled Uses of Network Management for Monitoring the "IP Packet Blocks Input Queue" PSIRT Advisory which details methods to identify impacted devices via SNMP, RMON, and Network Management products.

### Vendor Status:

Cisco has released software patches for the vulnerability and is available for download from the software center at:

<<http://www.cisco.com/tacpage/sw-center/>>  
<http://www.cisco.com/tacpage/sw-center/>

For software installation and upgrade procedures consult:

<[http://www.cisco.com/warp/public/130/upgrade\\_index.shtml](http://www.cisco.com/warp/public/130/upgrade_index.shtml)>  
[http://www.cisco.com/warp/public/130/upgrade\\_index.shtml](http://www.cisco.com/warp/public/130/upgrade_index.shtml)

Registered Cisco users can review all repaired images from:

<<http://www.cisco.com/tacpage/sw-center/sw-ios.shtml>>  
<http://www.cisco.com/tacpage/sw-center/sw-ios.shtml>

### Workarounds

There are three possible workarounds:

- \* Disabling the DHCP service

## Securiteam: [NEWS] Cisco IOS DHCP Blocked Interface DoS

- \* Control Plane Policing
- \* Two versions of Access Control Lists

### Disabling the DHCP Service

This vulnerability can be mitigated by utilizing the command:  
no service dhcp

However, this workaround will disable all DHCP processing on the device, including the DHCP helper functionality that may be necessary in some network configurations.

### Control Plane Policing Feature

The Control Plane Policy feature may be used to mitigate this vulnerability, as in the following example:

```
access-list 140 deny udp host 192.168.13.1 any eq bootps
access-list 140 deny udp any host 192.168.13.1 eq bootps
access-list 140 deny udp any host 255.255.255.255 eq bootps
access-list 140 permit udp any any eq bootps

class-map match-all bootps-class
match access-group 140

policy-map control-plane-policy
class bootps-class

    police 8000 1500 1500 conform-action drop exceed-action drop

control-plane
service-policy input control-plane-policy
```

Note: For this example 192.168.13.1 is a legitimate DHCP server.

Additional information on the configuration and use of the CPP feature can be found at this link:

[http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1838/products\\_feature\\_guide09186a00801afad4.html](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1838/products_feature_guide09186a00801afad4.html)

This workaround is only applicable to Cisco IOS 12.2S, as this feature is only available in Cisco IOS versions 12.2S and 12.3T. Cisco IOS 12.3T is not impacted by this advisory.

### Access Lists – Two Methods

Access lists can be applied to block DHCP/BootP traffic destined to any router interface addresses, as in the following example. In this example, the IP address 192.168.13.1 represents a legitimate DHCP server, the addresses 10.89.236.147 and 192.168.13.2 represent router interface addresses, and 192.168.61.1 represents a loopback interface on the router. Any bootp/dhcp packets destined to the router interface addresses are blocked.

## Securiteam: [NEWS] Cisco IOS DHCP Blocked Interface DoS

```
access-list 100 remark permit bootps from the DHCP server
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 remark deny bootps from any to router f1/0
access-list 100 deny udp any host 10.89.236.147 eq bootps
access-list 100 remark deny bootps from any to router f0/0
access-list 100 deny udp any host 192.168.13.2 eq bootps
access-list 100 remark deny bootps from any to router loopback1
access-list 100 deny udp any host 192.168.61.1 eq bootps
access-list 100 remark permit all other traffic
access-list 100 permit ip any any
```

Access-list 100 is applied to f0/0 and f1/0 physical interfaces.

```
interface FastEthernet0/0
ip address 192.168.13.2 255.255.255.0
ip access-group 100 in
interface FastEthernet1/0
ip address 10.89.236.147 255.255.255.240
ip access-group 100 in
ip helper-address 192.168.13.1
```

An alternate configuration for the interface access-list workaround. This example would also need to be applied to all physical interfaces, but deny statements for all of the IP addresses configured on the router are not necessary in this approach. In this example, the address 192.168.13.1 represents a legitimate DHCP server.

```
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 permit udp any host 192.168.13.1 eq bootps
access-list 100 permit udp any host 255.255.255.255 eq bootps
access-list 100 deny udp any any eq bootps
```

```
interface FastEthernet0/0
ip address 192.168.13.2 255.255.255.0
ip access-group 100 in
interface FastEthernet1/0
ip address 10.89.236.147 255.255.255.240
ip access-group 100 in
ip helper-address 192.168.13.1
```

Note: These workarounds will not prevent spoofed IP packets with the source IP address set to that of the DHCP server.

For more information on anti-spoofing refer to:

<[http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_tech\\_note09186a0080120f48.shtml#sec\\_ip](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#sec_ip)>  
[http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_tech\\_note09186a0080120f48.shtml#sec\\_ip](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#sec_ip)  
and  
<<http://www.ietf.org/rfc/rfc2827.txt>> <http://www.ietf.org/rfc/rfc2827.txt>

Securiteam: [NEWS] Cisco IOS DHCP Blocked Interface DoS

The Unicast Reverse Path Forwarding (Unicast RPF) feature helps to mitigate problems that are caused by spoofed IP source addresses. For further details, please refer to:

<[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur\\_c/fothersf/scfrpf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfrpf.htm)>  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur\\_c/fothersf/scfrpf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfrpf.htm)

ADDITIONAL INFORMATION

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

The original article can be found at:

<<http://www.cisco.com/warp/public/707/cisco-sa-20041110-dhcp.shtml>>  
<http://www.cisco.com/warp/public/707/cisco-sa-20041110-dhcp.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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.