

# Cisco Security Advisory: Cisco IOS DHCP Blocked Interface Denial-of-Service

Advisory ID: cisco-sa-20041110-dhcp

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

## Revision 1.2

Last Updated 2004 December 1 1500 UTC (GMT)

For Public Release 2004 November 10 1700 UTC (GMT)

---

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

---

## Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Impact](#)
- [Software Version and Fixes](#)
- [Workarounds](#)
- [Obtaining Fixed Software](#)
- [Exploitation and Public Announcements](#)
- [Status of this Notice: FINAL](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

---

## Summary

Cisco IOS® devices running branches of Cisco IOS version 12.2S 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. Cisco is providing free fixed software to address this issue. There are also workarounds to mitigate this vulnerability. This issue was introduced by the fix included in CSCdx46180 and is being tracked by Cisco Bug ID [CSCee50294](#) ( [registered](#) customers only) .

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20041110-dhcp.shtml>.

## ☐ Affected Products

This vulnerability was introduced by the fix for CSCdx46180, and was integrated in Cisco IOS 12.2(14)SZ and 12.2(18)S.

## ☐ Vulnerable Products

The following Cisco products running Cisco IOS version 12.2(14)SZ, or a variant of Cisco IOS 12.2(18)S (as listed in the following section) and higher are affected by this vulnerability.

- 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

This issue affects only Cisco devices running affected Cisco 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 and higher that do not have the configuration command **no service dhcp**. It is not necessary for DHCP server or relay agent to be configured in order for this vulnerability to be present and exploited; "service dhcp" is enabled by default in IOS and is the only setting necessary (in addition to interface addresses) for exploitation of this vulnerability. This includes routers as well as switches and line cards which run Cisco IOS software. Cisco devices which do not run Cisco IOS software are not affected. Cisco devices running affected Cisco IOS software with the command **no service dhcp** enabled are not affected.

To determine the software running on a Cisco product, log in to the device and issue the **show version** command to display the system banner. Cisco IOS software will identify itself as "Internetwork Operating System Software" or simply "IOS®." On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the IOS release name. Other Cisco devices will not have the **show version** command or will give different output.

The following example identifies a Cisco product running IOS release 12.0(3) with an installed image name of C2500-IS-L:

```
Cisco Internetwork Operating System Software IOS (TM)
2500 Software (C2500-IS-L), Version 12.0(3), RELEASE SOFTWARE
```

The release train label is "12.0."

The next example shows a product running Cisco IOS release 12.0(2a)T1 with an image name of C2600-JS-MZ:

```
Cisco Internetwork Operating System Software IOS (tm)
C2600 Software (C2600-JS-MZ), Version 12.0(2a)T1, RELEASE SOFTWARE (fc
```

Additional information about Cisco IOS release naming can be found at

<http://www.cisco.com/warp/public/620/1.html>.

## ☐ Products Confirmed Not Vulnerable

Cisco devices running affected Cisco IOS software with the command **no service dhcp** enabled are not affected.

Cisco products that run any versions of IOS **not** listed in the [Software Versions and Fixes](#) table below, are not affected.

Cisco products that do not run Cisco IOS software and are not affected by this vulnerability include, but are not limited to:

- 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.

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

## ☐ Details

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.

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.

```
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:
```

*!--- The 76/75 shows that this is blocked*

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

## ☐ Impact

A device receiving these specifically 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.

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

## ☐ Software Version and Fixes

Each row of the Cisco IOS software table below describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label). When selecting a release, keep in mind the following definitions:

- **Maintenance:** Most heavily tested, stable, and highly recommended release of a release train in any given row of the table.
- **Rebuild:** Constructed from the previous maintenance or major release in the same train, it contains the fix for a specific defect. Although it receives less testing, it contains only the minimal changes necessary to repair the vulnerability.

In all cases, customers should exercise caution to confirm that the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new software release. If the information is not clear, contact the Cisco

TAC for assistance as shown in the Obtaining Fixed Software section below.

More information on Cisco IOS software release names and abbreviations is available at <http://www.cisco.com/warp/public/620/1.html>.

The fixes will be available at the Software Center located at <http://www.cisco.com/tacpage/sw-center/>.

For software installation and upgrade procedures, see [http://www.cisco.com/warp/public/130/upgrade\\_index.shtml](http://www.cisco.com/warp/public/130/upgrade_index.shtml).

For a current view of all posted and repaired images for Cisco IOS, please check the listing available to registered Cisco.com users at: <http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438303> ( [registered](#) customers only) .

<b>Major Release</b>	<b>Availability of Repaired Releases</b>	
<b>Affected 12.2-Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
12.2(18)EW	12.2(18)EW2	
12.2(20)EW	Migrates to 12.2(20)EWA	
12.2(18)EWA		12.2(20)EWA
12.2(18)S	12.2(18)S6	
	12.2(20)S4	
	12.2(22)S2	
		12.2(25)S
12.2(18)SE	12.2(20)SE3	
12.2(18)SV		12.2(24)SV
12.2(18)SW		12.2(25)SW
12.2(18)SXD	Not impacted	
12.2(14)SZ	Migrates to 12.2(20)S4	

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

## ☐ Workarounds

There are four possible workarounds for this vulnerability:

- Disabling the dhcp service
- Control Plane Policing
- Two versions of Access Control Lists

The effectiveness of any workaround 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 is the most appropriate for use in the intended network before it is deployed.

### **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
```

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/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod\\_white\\_paper09](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper09)

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.

In this example, any bootp/dhcp packets destined to the router interface addresses are blocked.

```
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) and <http://www.ietf.org/rfc/rfc2827.txt> .

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/en/US/docs/ios/12\\_2/security/configuration/guide/scfrpf.html](http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfrpf.html).

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

## ☐ 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.

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

## ☐ 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>.

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

## ☐ 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.

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

## ☐ 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/en/US/support/tsd\\_cisco\\_worldwide\\_contacts.html](http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html) 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 public announcements or malicious use of the vulnerability described in this advisory.

This vulnerability was reported to Cisco by a customer.

## ☐ **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 will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20041110-dhcp.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](mailto:cust-security-announce@cisco.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto: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 1.2	2004-December-1	Updated Software version table - 12.2(20)EW.
Revision 1.1	2004-November-10	Added network review disclaimer text to Workaround section.
Revision 1.0	2004-November-10	Initial public release.

[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](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](#)

---

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)