

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)

Security Advisories

# Cisco Security Advisory: Cisco IOS Software Firewall Application Inspection Control Vulnerability

Advisory ID: **cisco-sa-20080924-iosfw**

<http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosfw.shtml>

## Revision 1.1

Last Updated 2009 April 16 2100 UTC (GMT)

For Public Release 2008 September 24 1600 UTC (GMT)

---

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

---

## Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Vulnerability Scoring 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

Cisco IOS software configured for IOS firewall Application Inspection Control (AIC) with a HTTP configured application-specific policy are vulnerable to a Denial of Service when processing a specific

malformed HTTP transit packet. Successful exploitation of the vulnerability may result in a reload of the affected device.

Cisco has released free software updates that address this vulnerability.

A mitigation for this vulnerability is available. See the "Workarounds" section for details.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosfw.shtml>.

**Note:** The September 24, 2008 IOS Advisory bundled publication includes twelve Security Advisories. Eleven of the advisories address vulnerabilities in Cisco's IOS software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each Advisory lists the releases that correct the vulnerability described in the Advisory.

Individual publication links are listed below:

- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosips.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ssl.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-cucm.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ipc.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-mfi.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ubr.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sccp.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosfw.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-l2tp.shtml>

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

## ☐ Affected Products

The HTTP AIC feature was introduced in Cisco IOS Software Release 12.4(9)T. The software table in this advisory identifies the affected releases.

## ☐ Vulnerable Products

Devices that are running a vulnerable version of Cisco IOS software and configured for Cisco IOS firewall AIC for HTTP are affected.

To determine the software running on a Cisco IOS product, log in to the device and issue the **show version** command-line interface (CLI) 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 Cisco IOS release name. Other Cisco devices will not have the **show version** command, or will give different output.

The following example shows output from a device running Cisco IOS image 12.4(15)T2:

```

router#show version
Cisco IOS Software, 1841 Software (C1841-ADVSECURITYK9-M),
  Version 12.4(15)T2, RELEASE SOFTWARE (fc7) Technical Support:
http://www.cisco.com/techsupport Copyright (c) 1986-2008 by Cisco
Systems, Inc. Compiled Thu 17-Jan-08 23:12 by prod_rel_team

!--- Output truncated.

```

Additional information on the Cisco IOS release naming conventions can be found on the document entitled "White Paper: Cisco IOS Reference Guide", which is available at <http://www.cisco.com/warp/public/620/1.html>.

The device is vulnerable if the configuration has a Layer 7 class map and Layer 7 policy map for HTTP deep packet inspection (DPI), and these policies are applied to any firewall zone. To determine whether the device is running a vulnerable configuration of Cisco IOS firewall AIC for HTTP, log in to the device and issue the CLI command **show policy-map type inspect zone-pair | section packet inspection**. If the output contains **Policy: http layer7-policymap name**, the device is vulnerable. The following example shows the response from a vulnerable device:

```

Router#show policy-map type inspect zone-pair | section packet inspection

      Deep packet inspection
        Policy: http layer7-policymap
          1 packets, 28 bytes

Router#

```

## ☐ Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by this vulnerability. IOS releases before 12.4(9)T are not affected by this issue. Products confirmed not vulnerable include:

- Cisco PIX
- Cisco ASA
- Cisco Firewall Services Module (FWSM)
- The Virtual Firewall (VFW) application on the multiservice blade (MSB) on the Cisco XR 12000 Series Router

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

## ☐ Details

Firewalls are networking devices that control access to an organization's network assets. Firewalls are often positioned at the entrance points into networks. Cisco IOS software provides a set of security features that enable you to configure a simple or elaborate firewall policy, according to your particular requirements.

HTTP uses port 80 by default to transport Internet web services, which are commonly used on the network and rarely challenged with regard to their legitimacy and conformance to standards. Because port 80 traffic is typically allowed through the network without being challenged, many application developers are leveraging HTTP traffic as an alternative transport protocol that will

allow their application's traffic to travel through or even bypass the firewall. When the Cisco IOS Firewall is configured with HTTP AIC, it performs packet inspection to detect HTTP connections that are not authorized in the scope of the security policy configuration. It also detects users who are tunneling applications through port 80. If the packet is not in compliance with the HTTP protocol, it will be dropped, the connection will be reset, and a syslog message will be generated, as appropriate.

Cisco IOS Software that is configured for IOS firewall AIC with an HTTP application-specific policy is vulnerable to a denial of service condition when it processes a specific malformed HTTP transit packet. Successful exploitation of the vulnerability may result in a reload of the affected device.

HTTP runs over TCP. For this vulnerability to be exploited, a full three-way handshake between client and server is required before any malicious traffic would be processed to result in a device reload.

Additional information regarding Cisco IOS Firewall AIC with HTTP application-specific policy maps is available at

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t6/htzonebp.htm>

This vulnerability is documented in Cisco bug ID [CSCsh12480](#) ([registered](#) customers only) and Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-3812 has been assigned to this vulnerability.

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

## ☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerability 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 2.0.

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

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

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>.

**CSCsh12480 - IOSFW with HTTP AIC may reload on processing crafted HTTP packet**

Calculate the environmental score of <a href="#">CSCsh12480</a>					
CVSS Base Score - <b>7.8</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - <b>6.4</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

## ▣ Impact

Successful exploitation of the vulnerability may result in a reload of the affected device. Repeated exploitation attempts may result in a sustained denial of service attack.

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

## ▣ 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.

Each row of the Cisco IOS software table (below) names a Cisco IOS release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (along with the anticipated date of availability for each, if applicable) are listed in the "First Fixed Release" column of the table. The "Recommended Release" column indicates the releases which have fixes for all the published vulnerabilities at the time of this Advisory. 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. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Releases" column of the table.

Major Release	Availability of Repaired Releases	
	First Fixed Release	Recommended Release
Affected 12.0-Based Releases		
There are no affected 12.0 based releases		

<b>Affected 12.1-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
There are no affected 12.1 based releases		
<b>Affected 12.2-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
There are no affected 12.2 based releases		
<b>Affected 12.3-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
There are no affected 12.3 based releases		
<b>Affected 12.4-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.4	Not Vulnerable	
12.4JA	Not Vulnerable	
12.4JK	Not Vulnerable	
12.4JL	Not Vulnerable	
12.4JMA	Not Vulnerable	
12.4JMB	Not Vulnerable	
12.4JMC	Not Vulnerable	
12.4JX	Not Vulnerable	
12.4MD	Not Vulnerable	
12.4MR	Not Vulnerable	
12.4SW	Not Vulnerable	
12.4T	Releases prior to 12.4 (9)T are not vulnerable. First fixed in:  12.4(9)T7  12.4(11)T4  12.4(15)T	12.4(15)T7
12.4XA	Not Vulnerable	
12.4XB	Not Vulnerable	
12.4XC	Not Vulnerable	

12.4XD	Not Vulnerable	
12.4XE	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
12.4XF	Not Vulnerable	
12.4XG	Not Vulnerable	
12.4XJ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
12.4XK	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(15)T7
12.4XL	Not Vulnerable	
12.4XM	Not Vulnerable	
12.4XN	Not Vulnerable	
12.4XP	Not Vulnerable	
12.4XQ	Not Vulnerable	
12.4XT	Not Vulnerable	
12.4XV	Vulnerable; contact TAC	
12.4XW	12.4(11)XW1	12.4(11)XW9
12.4XY	Not Vulnerable	
12.4XZ	Not Vulnerable	
12.4YA	Not Vulnerable	

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

## ☐ Workarounds

There are no known workarounds for this vulnerability. The only known action to help counter this vulnerability is to disable AIC HTTP deep packet inspection in the affected device's configuration. Disabling deep packet HTTP inspection will allow the rest of the firewall features to continue to function until a software upgrade can be implemented. All other firewall features will continue to perform normally.

### Disabling AIC HTTP Deep Packet Inspection

To disable AIC HTTP Deep Packet Inspection, remove the linkage between **policy-map type inspect layer4-policymap** and **policy-map type inspect http layer7-policymap**. This example shows an existing configuration, followed by how to remove AIC HTTP Deep Packet Inspection:

```
!--- Existing Configuration
!
```

```

parameter-map type inspect global

!

class-map type inspect http match-any layer7-classmap
class-map type inspect match-any layer4-classmap
  match protocol http

!

policy-map type inspect http layer7-policymap
  class type inspect http layer7-classmap
  allow
  class class-default
policy-map type inspect layer4-policymap
  class type inspect layer4-classmap
  inspect global
  service-policy http layer7-policymap
  class class-default

!

zone security inside
  description ** Inside Network **
zone security outside
  description ** Outside Network **
zone-pair security in2out source inside destination outside
  description ** Zone Pair - inside to outside **
  service-policy type inspect layer4-policymap

```

Remove the service-policy from the zone-pair in question:

```

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#zone-pair security in2out source inside destination outside
Router(config-sec-zone-pair)#no service-policy type inspect layer4-policymap
Router(config-sec-zone-pair)#exit

```

Remove the linkage between **policy-map type inspect layer4-policymap** and **policy-map type inspect http layer7-policymap**:

```

Router(config)#policy-map type inspect layer4-policymap
Router(config-pmap)#class type inspect layer4-classmap
Router(config-pmap-c)#no service-policy http layer7-policymap
Router(config-pmap-c)#exit
Router(config-pmap)#exit

```

Reapply the service-policy to the zone-pair in question:

```

Router(config)#zone-pair security in2out source inside destination outside
Router(config-sec-zone-pair)#service-policy type inspect layer4-policymap
Router(config-sec-zone-pair)#exit

```

Although not required, for completeness of the configuration the **policy-map type inspect http layer7-policymap** and **class-map type inspect http match-any layer7-classmap** are recommended to be removed.

```

Router(config)#no policy-map type inspect http layer7-policymap
Router(config)#no class-map type inspect http match-any layer7-classmap
Router(config)#exit
Router#

```

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

## ❑ Obtaining Fixed Software

Cisco has released free software updates that address this vulnerability. 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/en/US/docs/general/warranty/English/EU1KEN\\_.html](http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html), or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact 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 agreements 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 do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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)

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of 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 localized telephone numbers, and instructions and e-mail addresses for use in various languages.

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

## ☐ **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 found by Cisco internal testing.

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

## ☐ **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.

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

## ☐ **Distribution**

This advisory is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosfw.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-bulletins@lists.first.org](mailto:first-bulletins@lists.first.org)
- [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.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [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.

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

## ☐ Revision History

Revision 1.1	2009-April-16	Removed references to the combined software table, as it is now outdated
Revision 1.0	2008-September-24	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](#)

---

### Help us help you.

☐  
Please rate this document.

- ☐  Excellent  
 Good  
 Average  
 Fair  
 Poor

☐  
This document solved my problem.

- Yes
- No
- Just browsing

**Suggestions for improvement:**

(256 character limit)

<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.](#)