

# Cisco IOS Software Zone-Based Policy Firewall Vulnerability

Advisory ID: cisco-sa-20090923-ios-fw

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-ios-fw.shtml>

## Revision 1.0

For Public Release 2009 September 23 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<sup>®</sup> devices that are configured with Cisco IOS Zone-Based Policy Firewall Session Initiation Protocol (SIP) inspection are vulnerable to denial of service (DoS) attacks when processing a specific SIP transit packet. Exploitation of the vulnerability could result in a reload of the affected device.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-ios-fw.shtml>

**Note:** The September 23, 2009, Cisco IOS Security Advisory bundled publication includes eleven Security Advisories. Ten of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Advisory Bundled Publication" at the following link:

[http://www.cisco.com/web/about/security/intelligence/Cisco\\_ERP\\_sep09.html](http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html)

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

## ☐ Affected Products

This vulnerability affects a limited number of Cisco IOS Software releases. Consult the "Software Versions and Fixes" section of this advisory for the details of affected releases.

Only devices that are configured with Cisco IOS Zone-Based Policy Firewall SIP inspection (UDP port 5060, TCP ports 5060, and 5061) are vulnerable. Cisco IOS devices that are configured with legacy Cisco IOS Firewall Support for SIP (context-based access control (CBAC)) are not vulnerable.

## ☐ Vulnerable Products

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the **show version** command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the **show version** command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright © 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

<output truncated>
```

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.4(20)T with an installed image name of C1841-ADVENTERPRISEK9-M:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T,
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright © 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide" at the following link: <http://www.cisco.com/web/about/security/intelligence/ios-ref.html>

The device is vulnerable if the configuration has either a layer 3 or layer 7 SIP application-specific policy

configured, and these policies are applied to any firewall zone. To determine whether the device is running a vulnerable configuration, log in to the device and issue the command line interface (CLI) command **show policy-map type inspect zone-pair | include atch: access|protocol sip**. If the output contains "**Match: protocol sip**", the device is vulnerable. If the output contains **Match: access-group number**, then the device is only vulnerable if, the referenced access list permits the SIP protocol (UDP port 5060, or TCP ports 5060 and 5061). The following example shows a vulnerable device configured with Cisco IOS Zone-Based Policy Firewall SIP inspection:

```
Router#show policy-map type inspect zone-pair | include atch: access|protocol sip
      Match: protocol sip
Router#
```

The following example shows a vulnerable device configured with SIP inspection by way of an applied access list:

```
Router#show policy-map type inspect zone-pair | include atch: access|protocol sip
      Match: access-group 102
Router#
Router#show access-list 102
Extended IP access list 102
 10 permit udp any any eq 5060
 20 permit tcp any any eq 5060
 30 permit tcp any any eq 5061
Router#
```

A device that is not configured for SIP inspection or does not support this configuration will return either a blank line or an error message. The following is an example of a device that supports Cisco IOS Firewall but does not have SIP inspection enabled:

```
Router#show policy-map type inspect zone-pair | include atch: access|protocol sip
Router#
```

## ☐ Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by this vulnerability. Products confirmed not vulnerable include:

- Cisco PIX 500 Series Firewall
- Cisco ASA 5500 Series Adaptive Security Appliance
- Firewall Services Module (FWSM) for Catalyst 6500 Series Switches and 7600 Series Routers
- Virtual Firewall (VFW) application on the multiservice blade (MSB) on the Cisco XR 12000 Series Router
- Cisco ACE Application Control Engine Module
- Cisco IOS devices NOT configured with Cisco IOS Zone-Based Policy Firewall SIP inspection.
- Cisco IOS devices configured with legacy Cisco IOS Firewall Support for SIP (CBAC)
- Cisco IOS XE Software
- Cisco IOS XR Software

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

## ☐ Details

Firewalls are networking devices that control access to the network assets of an organization. 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.

SIP inspection in the Cisco IOS Firewall provides basic SIP inspect functionality (SIP packet inspection and pinhole opening) as well as protocol conformance and application security.

Cisco IOS Software that is configured with Cisco IOS Zone-Based Policy Firewall SIP inspection are vulnerable to a DoS attack when processing a specific SIP transit packet. Exploitation of this vulnerability will result in a reload of the affected device.

Cisco IOS Zone-Based Policy Firewall SIP inspection was first introduced in Cisco IOS Software versions 12.4(15)XZ and 12.4(20)T.

Cisco IOS Firewall CBAC support for SIP inspection by way of the **ip inspect name [inspection\_name] sip** is not vulnerable. Additional information regarding Cisco IOS Firewall CBAC support for SIP inspection is available in the document "Firewall Support for SIP" at the following link: [http://www.cisco.com/en/US/docs/ios/sec\\_data\\_plan\\_e/configuration/guide/sec\\_fw\\_all\\_sip\\_supp.html](http://www.cisco.com/en/US/docs/ios/sec_data_plan_e/configuration/guide/sec_fw_all_sip_supp.html)

Additional information regarding Cisco IOS Zone-Based Policy Firewall SIP inspection is available in the document "Cisco IOS Firewall: SIP Enhancements: ALG and AIC" at the following link: [http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec\\_sip\\_alg\\_aic.html](http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_sip_alg_aic.html)

This vulnerability is documented in the following Cisco Bug ID: [CSCsr18691](#) ( [registered](#) customers only) and has been assigned the Common Vulnerabilities and Exposures (CVE) identifier CVE-2009-2867.

[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>.

<b>CSCsr18691: Cisco IOS Software Zone-Based Policy Firewall Vulnerability</b>					
Calculate the environmental score of <a href="#">CSCsr18691</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 exploit attempts may result in a sustained DoS 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	
Affected 12.0-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.0 based releases		

Affected 12.1- Based Releases	First Fixed Release	Recommended Release
There are no affected 12.1 based releases		
Affected 12.2- Based Releases	First Fixed Release	Recommended Release
There are no affected 12.2 based releases		
Affected 12.3- Based Releases	First Fixed Release	Recommended Release
There are no affected 12.3 based releases		
Affected 12.4- Based Releases	First Fixed Release	Recommended Release
12.4	Not Vulnerable	
12.4GC	Not Vulnerable	
12.4JA	Not Vulnerable	
12.4JDA	Not Vulnerable	
12.4JDC	Not Vulnerable	
12.4JDD	Not Vulnerable	
12.4JK	Not Vulnerable	

12.4JL	Not Vulnerable	
12.4JMA	Not Vulnerable	
12.4JMB	Not Vulnerable	
12.4JX	Not Vulnerable	
12.4MD	Not Vulnerable	
12.4MDA	Not Vulnerable	
12.4MR	Not Vulnerable	
12.4SW	Not Vulnerable	
12.4T	Releases prior to 12.4(20)T are not vulnerable; 12.4(20)T2 12.4(22)T1 12.4(24)T	12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XA	Not Vulnerable	
12.4XB	Not Vulnerable	

12.4XC	Not Vulnerable	
12.4XD	Not Vulnerable	
12.4XE	Not Vulnerable	
12.4XF	Not Vulnerable	
12.4XG	Not Vulnerable	
12.4XJ	Not Vulnerable	
12.4XK	Not Vulnerable	
12.4XL	Not Vulnerable	
12.4XM	Not Vulnerable	
12.4XN	Not Vulnerable	
12.4XP	Not Vulnerable	
12.4XQ	Not Vulnerable	

12.4XR	Not Vulnerable	
12.4XT	Not Vulnerable	
12.4XV	Not Vulnerable	
12.4XW	Not Vulnerable	
12.4XY	Not Vulnerable	
12.4XZ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4YA	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4YB	12.4(22)YB4	12.4(22)YB4 12.4(22)YB5; Available on 19-OCT-2009
12.4YD	Not Vulnerable	
12.4YE	Not Vulnerable	

## ☐ Workarounds

The only workaround for this vulnerability is to disable Cisco IOS zone-based policy firewall SIP inspection in the affected device's configuration. Disabling SIP 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 SIP Inspection will vary depending on the implementation of the SIP inspection firewall.

[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\\_.htm](http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.htm), 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](mailto:psirt@cisco.com) or [security-alert@cisco.com](mailto: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/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 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 discovered 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-20090923-ios-fw.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.

## ☐ **Revision History**

Revision 1.0	2009-September-23	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](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>.

**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](#)

© 2010 - 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)