

# Cisco Security Advisory: Cisco Intrusion Prevention System Management Interface Denial of Service and Fragmented Packet Evasion Vulnerabilities

Advisory ID: [cisco-sa-20060920-ips](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20060920-ips.shtml>

## Revision 1.0

For Public Release 2006 September 20 1600 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 Intrusion Prevention System (IPS) software contains a denial of service vulnerability in web administration interface involving malformed Secure Socket Layer (SSL) packets and a fragmented packet evasion vulnerability.

There is a workaround for the web administration interface SSL denial of service vulnerability. There is no workaround for the fragmented packet IPS evasion vulnerability.

Cisco has made free software available to address these vulnerabilities for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20060920-ips.shtml>.

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

## ☐ Affected Products

This section provides details on affected products.

### ☐ Vulnerable Products

The following Cisco IPS/IDS versions are vulnerable to the web administration interface SSL denial of service issue:

- Cisco IDS 4.1(x) software prior to 4.1(5c)
- Cisco IPS 5.0(x) software prior to 5.0(6p1)
- Cisco IPS 5.1(x) software prior to 5.1(2)

The following Cisco IPS versions are vulnerable to the fragmented packet IPS evasion issue:

- Cisco IPS 5.0(x) software prior to 5.0(6p2)
- Cisco IPS 5.1(x) software prior to 5.1(2)

All platforms running vulnerable versions of Cisco IPS/IDS software are affected. This includes 4200 series appliances, IDSM2, NM-CIDS router modules, and ASA IPS modules (also referred to as Advanced Inspection and Prevention (AIP) Security Services Module [SSM]).

To determine the version of software running on an IPS/IDS device, log in to the IPS/IDS device via SSH or the console and issue the command **show version**.

```
sensor#show version
Application Partition: Cisco Intrusion
Prevention System, Version 5.1(2)S242.0
```

### ☐ Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

Cisco IOS<sup>®</sup> software images including the IPS feature set are not vulnerable to the IPS evasion vulnerability if Virtual Fragment Reassembly (VFR) is enabled. If VFR is not enabled, fragmented IP traffic is not inspected by the IPS component which may allow malicious traffic to evade detection. Please consult the IOS IPS documentation for more information.

[http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod\\_white\\_pap](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_pap)

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

## ☐ Details

Cisco Intrusion Prevention and Detection Systems are a family of network security devices that provide network-based threat prevention services.

The web administration interface of Cisco IPS/IDS devices contains a denial of service vulnerability. It is possible to send a malformed SSLv2 Client Hello packet to the IPS/IDS web administration interface, which may cause the process (mainApp) responsible for managing remote access to fail. This results in an IPS/IDS device becoming unresponsive to all future remote management requests through the web administration interface or the command-line interface (CLI) via SSH and the console. This vulnerability is documented in Cisco bug IDs [CSCsd91720](#) ( [registered](#) customers only) and [CSCsd92033](#) ( [registered](#) customers only) . This vulnerability was originally fixed in Cisco IPS version 5.1(2).

By using a specially crafted sequence of fragmented IP packets, it is possible for malicious traffic to evade inspection by a Cisco IPS device. This may allow an attacker to circumvent the protection provided by an IPS device and access internal systems. IPS devices running in inline and promiscuous modes are affected. This vulnerability is documented in Cisco bug IDs [CSCse17206](#) ( [registered](#) customers only) and [CSCsf12379](#) ( [registered](#) customers only) . This vulnerability was originally fixed in Cisco IPS version 5.1(2).

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

## ☐ Impact

Successful exploitation of the web administration interface SSL denial of service vulnerability may result in the failure of the mainApp process. If the mainApp process fails, the following tasks will cease operation:

- Reporting alerts to remote monitoring systems
- Automated modification of access control lists (ACLs) on remote firewall systems (PIX and IOS)
- Sending SNMP traps

Even though the mainApp has failed, the IPS/IDS device will continue to perform inspection of traffic for malicious activity. If configured, the device will continue to drop packets/connections inline and send TCP resets in response to any malicious activity. IPS/IDS devices must be rebooted to recover from this vulnerability. If an IPS/IDS device is configured with a service account, it is possible to log in to an affected device with the service account via SSH or the console and manually reboot the device.

Successful exploitation of the fragmented packet IPS evasion vulnerability may result in an attacker being able to evade detection by an IPS device. This could allow protected systems to be covertly attacked.

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

## ☐ Software Version 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) 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).

For more information on the terms "Rebuild" and "Maintenance," consult the following URL:

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

Affected Software Version	Fixed Software Version
Cisco IDS 4.1(5b) and earlier	Cisco IDS 4.1(5c)
Cisco IPS 5.0(6p1) and earlier	Cisco IPS 5.0(6p2)
Cisco IPS 5.1(1) and earlier	Cisco IPS 5.1(2)

**Note:** IPS version 5.1(2) is no longer available for download. It has been replaced by IPS version 5.1(3).

**Note:** Bug ID [CSCsd91720](#) ( [registered](#) customers only) is fixed in IPS version 5.0(6p1), and [CSCsf12379](#) ( [registered](#) customers only) is fixed in IPS version 5.0(6p2).

Fixed software for Cisco IPS versions 5.1(x) are available for download at <http://www.cisco.com/cgi-bin/tablebuild.pl/ips5?psrtdcat20e2> ( [registered](#) customers only) .

Fixed software for Cisco IPS versions 4.1(x) and 5.0(x) is available for download at <http://www.cisco.com/cgi-bin/tablebuild.pl/ids-patches?psrtdcat20e2> ( [registered](#) customers only) .

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

## ☐ Workarounds

It is possible to limit exposure to the web administration interface SSL denial of service vulnerability by applying an access control list (ACL) on an IPS/IDS device to restrict access to trusted management systems. Instructions to add an ACL can be found at:

<http://www.cisco.com/en/US/docs/security/ips/5.1/configuration/guide/idm/dmSetup.html#wp107>

There is no workaround for the fragmented packet IPS evasion vulnerability.

[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/warp/public/687/Directory/DirTAC.shtml> for additional TAC

contact information, including special 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.

The web administration interface SSL denial of service vulnerability was discovered by Charles McAuley of Imperfect Networks and Spirent Communications.

The fragmented packet IPS evasion vulnerability was reported to Cisco by Pratap Ramamurthy and Shai Rubin of the Wisconsin Safety Analyzer group (WiSA) in the Computer Science department at the University of Wisconsin.

[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-20060920-ips.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)
- [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 1.0	2006-August-20	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)

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

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

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