

Cisco Security Advisory: Cisco Intrusion Prevention System Jumbo Frame Denial of Service

Advisory ID: cisco-sa-20080618-ips

<http://www.cisco.com/warp/public/707/cisco-sa-20080618-ips.shtml>

Revision 1.0

For Public Release 2008 June 18 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 Intrusion Prevention System (IPS) platforms that have gigabit network interfaces installed and are deployed in inline mode contain a denial of service vulnerability in the handling of jumbo Ethernet frames. This vulnerability may lead to a kernel panic that requires a power cycle to recover platform operation. Platforms deployed in promiscuous mode only or that do not contain gigabit network interfaces are not vulnerable.

Cisco has released free software updates that address this vulnerability. There is a workaround for this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080618-ips.shtml>.

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

☐ Affected Products

☐ Vulnerable Products

The following Cisco IPS versions are affected:

- Cisco Intrusion Prevention System version 5.x prior to 5.1(8)E2
- Cisco Intrusion Prevention System version 6.x prior to 6.0(5)E2

The following Cisco IPS platforms ship with gigabit network interfaces and are vulnerable if they are deployed in inline mode:

- 4235
- 4240
- 4250
- 4250SX *
- 4250TX
- 4250XL *
- 4255
- 4260
- 4270

* The 4250SX and 4250XL models ship with gigabit network interfaces that are normally used for remote administration and monitoring. If the gigabit network interfaces are configured for use with inline mode, the platform is vulnerable.

To determine the version of software that is running on a Cisco IPS platform, log into the platform using the console or Secure Shell (SSH) and issue the **show version** command.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 6.0(4a)E1
```

To determine whether a Cisco IPS platform has interfaces configured for inline mode, log into the platform using the console or SSH and issue the **show interfaces** command. Look for paired interfaces in the Inline Mode statement of the command output.

```
sensor# show interfaces
...
MAC statistics from interface GigabitEthernet0/1
  Interface function = Sensing interface
  Description =
  Media Type = TX
  Missed Packet Percentage = 0
  Inline Mode = Paired with interface
GigabitEthernet0/0
...
MAC statistics from interface GigabitEthernet0/0
  Interface function = Sensing interface
  Description =
  Media Type = TX
  Missed Packet Percentage = 0
  Inline Mode = Paired with interface
GigabitEthernet0/1
```

☐ Products Confirmed Not Vulnerable

The following Cisco IPS platforms are not vulnerable:

- 4210
- 4215
- SSM-AIP10
- SSM-AIP20

- SSM-AIP40
- AIM-IPS
- NM-CIDS
- IDSM2

Cisco IPS version 6.1(1) is not vulnerable. Cisco IOS with the Intrusion Prevention System feature is not vulnerable. No other Cisco products are currently known to be affected by this vulnerability.

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

☐ Details

Certain Cisco IPS platforms contain a denial of service vulnerability in the handling of jumbo ethernet frames. When a specific series of jumbo Ethernet frames is received on a gigabit network interface of a vulnerable Cisco IPS platform that is deployed in inline mode, a kernel panic may occur that results in the complete failure of the platform and causes a network denial of service condition. Cisco IPS platforms that are deployed in promiscuous mode only or that do not contain gigabit network interfaces are not vulnerable.

Jumbo Ethernet support is usually deployed in data center environments to increase inter-server communication performance and is not a default configuration for Cisco routers and switches. Support for jumbo Ethernet frames must be enabled on each device that require the feature. In order to exploit this vulnerability, an attacker must be able to inject jumbo Ethernet frames to a vulnerable Cisco IPS platform that is deployed in inline mode.

If they are configured to use bypass mode to allow traffic to pass in the event of a system failure, all Cisco IPS platforms will fail to forward traffic except for the 4260 and 4270 platforms. The Cisco IPS 4260 and 4270 platforms contain a hardware bypass feature that allows them to pass network traffic in the event of a kernel panic or power outage. They will pass traffic by default if the hardware bypass feature is engaged.

This vulnerability is documented in Cisco Bug ID CSCso64762 and has been assigned Common Vulnerabilities and Exposures (CVE) ID [CVE-2008-2060](#).

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

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities 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>.

<u>CSCso64762 - IPS Jumbo frame not processed properly (registered customers only)</u>					
Calculate the environmental score of <u>CSCso64762</u>					
CVSS Base Score - 7.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	Partial	None	Complete
CVSS Temporal Score - 6.4					
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 network denial of service condition. A power cycle is required to recover operation. An attacker may be able to evade access controls and detection of malicious activity in the case of Cisco IPS 4260/4270 platforms that have hardware

bypass configured to pass traffic in the event of a kernel panic.

[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.

This vulnerability is fixed in Cisco IPS versions 5.1(8)E2 and 6.0(5)E2 that are expected to be available for download by June 20, 2008.

Fixed software Cisco IPS version 5.1(8)E2 will be available at the following link:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ips5?psrtdcat20e2>

Fixed software Cisco IPS version 6.0(5)E2 will be available at the following link:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ips6?psrtdcat20e2>

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

☐ **Workarounds**

To workaround this vulnerability, administrators can disable jumbo Ethernet support on routers and switches directly that are connected to vulnerable Cisco IPS platforms. This workaround may produce a negative performance impact in certain environments. Administrators are encouraged to upgrade to fixed software.

For more information about configuring Jumbo frames on Cisco switches, please reference the following link:

http://www.cisco.com/en/US/products/hw/switches/ps700/products_configuration_example09186a008010edab.shtml

☐ **Obtaining Fixed Software**

Cisco has released free software updates that address these vulnerabilities. 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, 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

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 reported to Cisco by HD Moore of BreakingPoint Systems.

[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-20080618-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
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- 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	2008-June-18	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. 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)



[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)