

Cisco Security Advisory: Cisco Intrusion Prevention System Malformed Packet Denial of Service

Advisory ID: cisco-sa-20060712-ips

<http://www.cisco.com/warp/public/707/cisco-sa-20060712-ips.shtml>

Revision 1.0

For Public Release 2006 July 12 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 version 5.1 is vulnerable to a denial of service condition caused by a malformed packet, which may result in an IPS device becoming inaccessible remotely or via the console and fail to process packets. A power reset is required to recover the IPS device. There are no workarounds for this vulnerability.

Cisco has made free software available to address this vulnerability for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20060712-ips.shtml>.

Affected Products

Vulnerable Products

Cisco Intrusion Prevention System 42xx appliances running IPS software versions 5.1(1), 5.1(1a), 5.1(1b), 5.1(1c), 5.1(1d), 5.1(1e) or 5.1(p1).

IPS software versions 5.1(1a), 5.1(1b), 5.1(1c), 5.1(1d) and 5.1(1e) are repackaged versions of 5.1(1) created to fix various installation problems. All 5.1(1) patch versions report 5.1(1) as the installed version.

Note: Some IDS/IPS appliances shipped before IPS software version 5.0 was available and have model numbers starting with IDS, not IPS.

The following 42xx appliances are potentially affected.

- IDS-4235
- IPS-4240
- IDS-4250-SX
- IDS-4250-TX
- IDS-4250-XL (4250 with XL accelerator card)
- IPS-4255

Products Confirmed Not Vulnerable

All devices running Cisco Intrusion Detection Systems (IDS) software versions 4.x or IPS versions 5.0(x).

Additionally, the following devices are not vulnerable even if running IPS software versions 5.1(1), 5.1(1a), 5.1(1b), 5.1(1c), 5.1(1d), 5.1(1e) or 5.1(1p1).

- NM-CIDS
- IDSM-2
- ASA-SSM-AIP-10
- ASA-SSM-AIP-20

- IDS-4210
- IDS-4215

The following devices do not support IPS software version 5.1 and are not vulnerable.

- IDS-4220
- IDS-4230

To determine the version of software running an IPS device, log into the IPS device using an SSH client and issue the command **show version**.

```
sensor#show version  
Application Partition: Cisco Intrusion  
Prevention System, Version 5.1(1p1)S215.0
```

Details

Cisco Intrusion Prevention Systems (IPS) are a family of network security devices that provide network based threat prevention services. A vulnerability exists in the custom device driver for Intel-based gigabit network adapters used to process packets received by the sensing interfaces of certain IPS devices. A malformed IP packet received on an Intel-based gigabit network adapter configured for use as a sensing interface may result in the IPS device experiencing a kernel panic. Affected IPS devices will cease processing packets, producing alerts, performing automated actions such as logging, and become inaccessible remotely or via the console.

If deployed as an inline device, the IPS will also stop forwarding packets between interfaces and may cause a network outage. IPS devices configured to use the auto-bypass feature will also fail to forward packets. Attackers may use this vulnerability to disable an IPS device to hide malicious activity. This vulnerability only affects certain IPS devices configured to use Intel-based gigabit network adapters as sensing interfaces. IPS devices configured to use an Intel-based gigabit network adapter as a management interface are not affected by this vulnerability. A power reset is required to recover the IPS device.

This vulnerability is documented in Cisco bug ID [CSCsd36590](#) ([registered](#) customers only) .

Impact

Successful exploitation of the vulnerability may result in the failure of an IPS device to operate as expected. Affected devices will become inaccessible remotely or via the console and stop processing packets. If deployed as an inline device, an IPS device will stop forwarding packets, including devices configured to use the auto-bypass feature. This may result in a network outage. A power reset is required to recover the IPS device.

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.

This issue is fixed in IPS version 5.1(2) which is available for download at <http://www.cisco.com/cgi-bin/tablebuild.pl/ips5> ([registered](#) customers only) .

Workarounds

There are no workarounds for this vulnerability.

Obtaining Fixed Software

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. 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.

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 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.

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

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.

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

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 is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20060712-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.

Revision History

Revision 1.0	2006-July-12 1600 UTC (GMT)	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. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 1992-2006 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).