

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

Cisco Security Advisory: Cisco Intrusion Prevention System Vulnerable to Privilege Escalation

Revision 1.0

For Public Release 2005 August 22 1700 UTC (GMT)

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

Contents

[Summary](#)[Affected Products](#)[Details](#)[Impact](#)[Software Versions and Fixes](#)[Obtaining Fixed Software](#)[Workarounds](#)[Exploitation and Public Announcements](#)[Status of This Notice: FINAL](#)[Distribution](#)[Revision History](#)[Cisco Security Procedures](#)

Summary

Cisco Intrusion Prevention Systems (IPS) are a family of network security devices that provide network based threat prevention services.

A user with OPERATOR or VIEWER access privileges may be able to exploit a vulnerability in the command line processing (CLI) logic to gain full administrative control of the IPS device.

Cisco has made free software available to address this vulnerability.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20050824-ips.shtml>

Affected Products

Vulnerable Products

Cisco Intrusion Prevention System version 5.0(1) and 5.0(2).

Products Confirmed Not Vulnerable

Any Cisco Intrusion Detection Systems (IDS) or IPS version 4.x and earlier.

Details

A user with OPERATOR or VIEWER access privileges may be able to exploit a vulnerability in the command line processing logic to gain full administrative control of the IPS device. OPERATOR and VIEWER accounts are normally non-privileged accounts used for monitoring and troubleshooting purposes.

This vulnerability is documented in the Cisco Bug Toolkit as Bug ID [CSCsb16527](#) ([registered](#) customers only)

Impact

Successful exploitation of this vulnerability grants an attacker full control of the IPS Device.

With full administrative access, an attacker may use the IPS device to bypass intrusion detection logic, run arbitrary code or perform a denial of service attack on the network and/or IPS device.

If the IPS device is used in inline mode, an attacker may cause an interruption of network service.

Software Versions and Fixes

This issue is fixed in IPS version 5.0(3) which is available for download at <http://www.cisco.com/cgi-bin/tablebuild.pl/ips5>

Obtaining Fixed Software

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 assistance with the upgrade, which should be free of charge.

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

Please 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.

Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

See <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.

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>.

Workarounds

As a security best practice, you should always configure your IPS device with a list of trusted hosts or networks that you want to have access to the IPS sensor.

For more information on setting up IPS access lists so that only trusted hosted and networks may access the sensor, please see

http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_configuration_guide_chapter09186a008045a77c.html#wp1031536

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 issue was discovered during internal testing.

Status of This Notice: FINAL

THIS ADVISORY IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTY OF MERCHANTABILITY. YOUR USE OF THE INFORMATION ON THE ADVISORY OR MATERIALS LINKED FROM THE ADVISORY IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS NOTICE AT ANY TIME.

A stand-alone copy or paraphrase of the text of this security advisory 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 will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20050824-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 (includes CERT/CC)
- bugtraq@securityfocus.com
- 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	2005-August-22	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>.

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)

Send

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

All contents are Copyright © 1992-2005 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).