

# Cisco Security Advisory: Multiple Vulnerabilities Found by PROTOS IPSec Test Suite

Document ID: 68158

Advisory ID: cisco-sa-20051114-ipsec

<http://www.cisco.com/warp/public/707/cisco-sa-20051114-ipsec.shtml>

## Revision 1.9

**Last Updated** 2006 January 12 1630 UTC (GMT)

For Public Release 2005 November 14 1100 UTC (GMT)

---

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

---

[Summary](#)

[Affected Products](#)

[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

Multiple Cisco products contain vulnerabilities in the processing of IPSec IKE (Internet Key Exchange) messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) "PROTOS" Test Suite for IPSec and can be repeatedly exploited to produce a denial of service.

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.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051114-ipsec.shtml>.

## Affected Products

This section provides details on affected products.

## Vulnerable Products

Cisco devices running affected versions of software and configured for IKE are vulnerable. This vulnerability is not dependent on a specific hardware configuration. For example, the Cisco VPN SM or VPN SPA are not required for the device to be vulnerable.

- Cisco IOS versions based on 12.2SXD, 12.3T, 12.4 and 12.4T
- Cisco PIX Firewall versions up to but not including 6.3(5)
- Cisco PIX Firewall/ASA versions up to but not including 7.0.1.4
- Cisco Firewall Services Module (FWSM) versions up to but not including 2.3(3)
- Cisco VPN 3000 Series Concentrators versions up to but not including 4.1(7)H and 4.7(2)B
- Cisco MDS Series SanOS versions up to but not including 2.1(2)
- Cisco Wireless LAN Controllers up to and including 3.2.78.0 with Crypto Accelerator present.

To determine the software running on a Cisco IOS product, log in to the device and issue the show version command to display the system banner. Cisco IOS software will identify itself as "Internetwork Operating System Software" or simply "IOS." On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the Cisco IOS release name. Other Cisco devices will not have the show version command, or will give different output.

The following example identifies a Cisco 7200 router running Cisco IOS release 12.3(10a) with an installed image name of C7200-JO3S-M.

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-JO3S-M), Version 12.3(10a), RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2004 by cisco Systems, Inc.
```

Additional information about Cisco IOS release naming can be found at <http://www.cisco.com/warp/public/620/1.html>.

Only Cisco IOS images that contain the Crypto Feature Set contain the vulnerable IPSec code. Customers that are not running an IOS image with crypto support are not exposed to this vulnerability.

Cisco IOS feature set naming indicates that IOS images with crypto support will have 'K8' or 'K9' in the feature designator field.

For example, the image in the example above, C7200-JO3S-M, does not contain 'K8' or 'K9.' This indicates that this image does not support crypto, and is therefore not vulnerable to the issues described in this Security Advisory.

The following output was taken from a device that is running an IOS image with crypto support:

```
Cisco Internetwork Operating System Software
IOS (tm) c6sup2_rp Software (c6sup2_rp-PK9S-M), Version 12.2(18)SXD5, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Fri 13-May-05 21:12 by ssearch
```

Since the feature set designator (PK9S) contains 'K9', we can quickly determine that this feature set contains crypto support.

## Products Confirmed Not Vulnerable

No other IOS trains are known to be affected.

Cisco IOS XR is not affected.

Cisco wireless LAN controllers without Crypto Accelerator present.

Cisco Catalyst 6500 Series Wireless Services Module.

Cisco Wireless LAN Controller Module for Integrated Services Routers.

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

## Details

IP Security, or IPSec, is a set of protocols standardized by the IETF to support encrypted and/or authenticated transmission of IP packets. IPSec is a protocol commonly used in Virtual Private Networks (VPNs).

The Internet Key Exchange (IKE) protocol is used to negotiate keying material for IPSec Security Associations (SAs) and provides authentication of peers.

For more complete information on IPSec, consult IETF Request For Comments (RFCs) 2401:

<http://www.ietf.org/rfc/rfc2401.txt>

For more complete information on IKE, consult IETF Request For Comments (RFCs) 2408 and 2409:

<http://www.ietf.org/rfc/rfc2408.txt>

<http://www.ietf.org/rfc/rfc2409.txt>

IPSec is used in two general cases.

The first case is LAN-to-LAN VPN operation in which two devices negotiate an IPSec connection between them for the purposes of connecting two remote LANs via an IPSec tunnel. In this case the devices negotiating the IPSec connection generally have static IP addresses, and the IPSec tunnel is up as long as there is traffic that needs to traverse the tunnel.

The second case is a Remote Access (RA) VPN which is typically used to allow remote clients a connection to a secure network or service. A common example of this is a user connecting to a corporate network while away from the office. In this scenario, the remote user could be connecting from anywhere, and their IP address is not static, but rather dynamically assigned via the transport provider.

IKE is not a requirement for the establishment of IPSec connections. Depending on your requirements and the devices involved, it may be possible to statically configure the SA information and disable IKE. This type of configuration may not be possible in the case of RA VPNs due to the user's IP address being unknown prior to the establishment of the IPSec connection. See the Workarounds Section for more information.

The PROTOS test suite for IPSec is designed to test the design limits of IPSec implementations by sending malformed IKE messages to the target device.

When receiving certain malformed packets, vulnerable Cisco devices may reset, causing a temporary Denial

of Service (DoS).

The vulnerabilities identified can be easily and repeatedly reproduced with the use of the OUSPG "PROTOS" Test Suite for IKE. This suite is designed to test the design limits of implementations that process IKE messages.

## Additional Details for Cisco IOS

The vulnerabilities addressed by this Advisory were introduced in IOS version 12.3(4)T, and are present in versions of 12.3T, 12.4, 12.4T, and 12.2SXD.

Prior to IOS version 12.3(8)T, IKE was enabled by default, with no crypto configuration needed for the IOS device to process IKE messages.

12.2SXD versions of Cisco IOS have IKE enabled by default. To ensure that IKE processing is disabled, enter the global configuration command **no crypto isakmp enable**.

As of IOS version 12.3(8)T (which includes all 12.4-based versions), crypto configuration is required to enable IKE message processing.

In order for an IOS device to process IKE packets, a crypto map must be configured and applied to an interface.

## Additional Details for Cisco PIX

The Cisco PIX does not enable IKE processing by default in any versions of software.

For Cisco PIX versions prior to 7.0, use the following to determine if IKE message processing is enabled:

```
show isakmp enable
```

The following example shows the output when IKE is enabled on the outside interface:

```
pixfirewall(config)# show isakmp enable  
isakmp enable outside
```

The following example shows the output when IKE is not enabled on any interface:

```
pixfirewall(config)# show isakmp  
pixfirewall(config)#
```

For Cisco PIX/ASA versions 7.0 and later, IKE is enabled only if the following command is in the device configuration:

```
isakmp enable
```

## Additional Details for Cisco Wireless LAN controllers

The Cisco Wireless LAN controllers do not enable IKE message processing by default in any versions of software and requires a Crypto Accelerator card to be present in the controller to allow configuration of IPsec and IKE message processing.

To determine if IKE message processing is enabled from the CLI prompt issue the command:

```
show wlan <wlan identifier>
```

In a system where IKE message processing is enabled, IP Security field will be marked "Enabled" and IKE configuration information will be present in the **show wlan <wlan ID>** output.

The following example shows the output when IKE message processing is enabled on WLAN 1:

```
(WLC) >show wlan 1

WLAN Identifier..... 1
Network Name (SSID)..... mobile
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Network Access Control..... Disabled
Number of Active Clients..... 1
Exclusionlist Timeout..... 60 seconds
Session Timeout..... Infinity
Interface..... management
DHCP Server..... 10.1.1.3
DHCP Address Assignment Required..... Enabled
Quality of Service..... Silver (best effort)
WMM..... Disabled
802.11e..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
IPv6 Support..... Disabled
Radio Policy..... All
Security
  802.11 Authentication:..... Open System
  Static WEP Keys..... Disabled
  802.1X..... Disabled
  Wi-Fi Protected Access (WPA1)..... Disabled
  Wi-Fi Protected Access v2 (WPA2)..... Disabled
  IP Security..... Enabled
    Authentication:..... HMAC-SHA-1
    Encryption:..... 3DES
    AH:..... Disabled (not changeable)
    IKE Authentication:..... Pre-Shared-Key
      Pre-Shared Key Length:..... 8 bytes
    IKE Diffie Hellman Group:..... DH Group 2 (1024 bits)
    IKE Phase 1 Mode:..... Aggressive
    PFS Key Mode:..... Disabled (not changeable)
    IKE Timeout:..... 57600 seconds

  IP Security Passthru..... Disabled
  L2TP..... Disabled
  Web Based Authentication..... Disabled
  Web-Passthrough..... Disabled
  Auto Anchor..... Disabled
  Cranite Passthru..... Disabled
  Fortress Passthru..... Disabled
```

In a system where IKE message processing is not enabled, IP Security field will be marked "Disabled" and IKE configuration information will not be present in the **show wlan <wlan ID>** output.

The following example shows the output when IKE message processing is not enabled on any WLAN interface:

```
(WLC) >show wlan 1

WLAN Identifier..... 1
Network Name (SSID)..... Airespace1
Status..... Disabled
MAC Filtering..... Disabled
```

```

Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Network Access Control..... Disabled
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
Interface..... management
DHCP Server..... Default
Quality of Service..... Silver (best effort)
WMM..... Disabled
802.11e..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
IPv6 Support..... Disabled
Radio Policy..... All
Security
  802.11 Authentication:..... Open System
  Static WEP Keys..... Disabled
  802.1X..... Enabled
    Encryption:..... 104-bit WEP
  Wi-Fi Protected Access (WPA1)..... Disabled
  Wi-Fi Protected Access v2 (WPA2)..... Disabled
  IP Security..... Disabled
  IP Security Passthru..... Disabled
  L2TP..... Disabled
  Web Based Authentication..... Disabled
  Web-Passthrough..... Disabled
  Auto Anchor..... Disabled
  Cranite Passthru..... Disabled
  Fortress Passthru..... Disabled

```

## Cisco Bug IDs

Below are the Cisco bug IDs and their corresponding product(s):

- Cisco IOS versions based on 12.2SX, 12.3T, 12.4 and 12.4T – [CSCed94829](#) ([registered](#) customers only)
- Cisco PIX Firewall versions up to but not including 6.3(5) – [CSCei14171](#) ([registered](#) customers only)
- Cisco PIX Firewall/ASA versions up to but not including 7.0.1.4 – [CSCei15053](#) ([registered](#) customers only)
- Cisco Firewall Services Module (FWSM) versions up to but not including 2.3(3) – [CSCei19275](#) ([registered](#) customers only)
- Cisco VPN 3000 Series Concentrators versions up to but not including 4.1(7)H and 4.7(2)B – [CSCsb15296](#) ([registered](#) customers only)
- Cisco MDS Series SanOS versions up to but not including 2.1(2) – [CSCei46258](#) ([registered](#) customers only)
- Cisco Wireless LAN controllers up to and including 3.2.78.0 – [CSCsc75655](#) ([registered](#) customers only)

## Impact

Successful exploitation of the vulnerability on the Cisco MDS Series may result in the restart of the IKE process. All other Cisco MDS device operations will continue normally.

Successful exploitation of the vulnerabilities on all other Cisco devices may result in the restart of the device. The device will return to normal operation without any intervention required.

## 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.

## Non-IOS Products

Affected Product	Vulnerable Version	Fixed Version
Cisco PIX running pre-7.0 code	Up to, but not including, 6.3(5)	6.3(5) or later
Cisco PIX/ASA running 7.0 or later code	Up to, but not including 7.0.1.4	7.0.1.4 or later
Cisco FWSM for Catalyst 6500 or 7600	Up to, but not including, 2.3(3)	2.3(3) or later
Cisco VPN3000 Concentrators running pre 4.7 code	Up to, but not including, 4.1(7)H	4.1(7)H or later
Cisco VPN3000 Concentrators running 4.7 code	Up to, but not including, 4.7(2)B	4.7(2)B or later
Cisco MDS devices	Up to, but not including, 2.1(2)	2.1(2) or later
Cisco Wireless LAN controller	Up to, and including 3.2.78.0	Vulnerable, contact TAC

## Cisco IOS

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 further information on the terms "Rebuild" and "Maintenance," please consult the following URL: <http://www.cisco.com/warp/public/620/1.html>

For Cisco IOS, the vulnerabilities were introduced with 12.3(4)T and 12.2(18)SXD. Previous versions of Cisco IOS are not affected.

Major Release	Availability of Repaired Releases	
<b>Affected 12.2-Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>

12.2SXD	12.2(18)SXD7; available 13-Dec-05	
<b>Affected 12.3-Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
12.3T	12.3(4)T12: Vulnerable; migrate to 12.4(5) or later	
	12.3(11)T9; available 27-Dec-05	
	12.3(14)T5	
12.3TPC	<del>Vulnerable; contact TAC</del>	
12.3XD	Vulnerable; migrate to 12.3(14)T5 or later	
12.3XE	Vulnerable. For C820v and SOHO78, migrate to 12.4(5) or later. For all other platforms, contact TAC.	
12.3XF	Vulnerable; migrate to 12.3(14)T5 or later	
12.3XG	Vulnerable. For C828, C820v, and SOHO78, migrate to 12.4(5) or later. For all other platforms, contact TAC.	
12.3XH	<del>Vulnerable; contact TAC</del>	
12.3XI	<del>Vulnerable; contact TAC</del>	
12.3XJ	Vulnerable: migrate to 12.3(14)YX; available 22-Dec-05	
12.3XK	<del>Vulnerable; contact TAC</del>	
12.3XM	Vulnerable; migrate to 12.3(14)T5 or later	
12.3XQ	Vulnerable; migrate to 12.4(5) or later	
12.3XR	Vulnerable. For C820v, C828, and SOHO78, migrate to 12.4(5) or later. For all other platforms, contact TAC.	
12.3XS	Vulnerable; migrate to 12.4(5) or later	
12.3XU	Vulnerable; migrate to 12.4(4)T or later	
12.3XW	Vulnerable: migrate to 12.3(14)YX; available	

	22-Dec-05	
12.3XX	Vulnerable; migrate to 12.4(5) or later	
12.3YA	Vulnerable. For C828, migrate to 12.4(5) or later. For all other platforms, contact TAC.	
12.3YD	Vulnerable; migrate to 12.4(4)T or later	
12.3YF	Vulnerable; migrate to 12.3(14)YX; available 22-Dec-05	
12.3YG	Vulnerable; contact TAC	
12.3YH	Vulnerable; contact TAC	
12.3YI	Vulnerable; contact TAC	
12.3YJ	Vulnerable; migrates to 12.3(14)YQ4, available 1-Dec-05	
12.3YK	Vulnerable; migrate to 12.4(4)T	
12.3YM	12.3(14)YM4	
12.3YQ	12.3(14)YQ4; available 01-Dec-05	
12.3YS	Vulnerable; contact TAC	
12.3YT	Vulnerable; migrate to 12.4(4)T	
12.3YU	Vulnerable; contact TAC	
12.3YX	Vulnerable; contact TAC	
<b>Affected 12.4-Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
12.4	12.4(1c); available 14-Nov-05	
	12.4(3b); available 12-Dec-05	
		12.4(5)
12.4T	12.4(2)T2	
		12.4(4)T
12.4XA	Vulnerable; contact TAC	
12.4XB		12.4(2)XB; available TBD

# Workarounds

The effectiveness of any workaround 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 is the most appropriate for use in the intended network before it is deployed.

For customers that use IPSec, but do not require IKE for connection establishment, IPSec connection information may be able to be entered manually, and IKE can be disabled, eliminating the exposure.

Note: Due to the potential complexity of configuring IPSec information, this is likely not a viable alternative for most customers, but is mentioned here for completeness. Please consult your product documentation for further information on static IPSec configuration.

## Restricting IKE Messages

It is possible to mitigate the effects of this vulnerability by restricting the devices that can send IKE traffic to your IPSec devices. Due to the potential for IKE traffic to come from a spoofed source address, a combination of Access Control Lists (ACLs) and anti-spoofing mechanisms will be most effective.

## Anti-spoofing

The Unicast Reverse Path Forwarding (Unicast RPF) feature helps to mitigate problems that are caused by spoofed IP source addresses. It is available on Cisco routers and firewalls. For further details, please refer to:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur\\_c/fothersf/scfrpf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfrpf.htm)

By enabling Unicast Reverse Path Forwarding (uRPF), all spoofed packets will be dropped at the first device. To enable uRPF, use the following commands.

```
router(config)# ip cef
router(config)# interface <interface #>
router(config-if)# ip verify unicast reverse-path
```

## Infrastructure Access Control Lists

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The white paper "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection ACLs:

<http://www.cisco.com/warp/public/707/iacl.html>.

## 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.

## 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](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.

## Exploitation and Public Announcements

The OUSPG Test Suite for IPSec can be used to trigger these vulnerabilities.

These vulnerabilities were discovered in cooperation with CERT-FI and NISCC. For their release information, please see <http://www.niscc.gov.uk/niscc/vulnAdv-en.html>.

## 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-20051114-ipsec.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 1.9	12-January-2006	Updated the Vulnerable Products section. Updated the Products Confirmed Not Vulnerable section. Add the Additional Details for Cisco Wireless LAN controllers section. Updated the Cisco Bug IDs section. Updated the Software Versions and Fixes section Non-IOS products table.
Revision 1.8	11-January-2006	Removed "12.3(7)T13" and "12.3(8)T12" from the Cisco IOS table under Software Versions and Fixes.
Revision 1.7	15-December-2005	Updated Cisco IOS Products table and changed the availability date of 12.3(11)T9 to 27-Dec-05.
Revision 1.6	06-December-2005	Updated Additional Details for Cisco IOS section. Updated

		Cisco IOS section.
Revision 1.5	<del>29–November–2005</del>	Updated Cisco IOS Products table.
Revision 1.4	<del>17–November–2005</del>	Updated Cisco IOS Products table.
Revision 1.3	<del>15–November–2005</del>	Updated Non–IOS Products table.
Revision 1.2	<del>15–November–2005</del>	Updated Advisory Id.
Revision 1.1	14–November–2005	Updated Non–IOS Products table. Updated command output in the Additional Details for Cisco PIX section. Updated Additional Details for Cisco IOS section.
Revision 1.0	<del>14–November–2005</del>	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>.

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jan 12, 2006

Document ID: 68158

---