

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

Security Advisories

Cisco Security Advisory: Cisco 10000, uBR10012, uBR7200 Series Devices IPC Vulnerability

Advisory ID: [cisco-sa-20080924-ipc](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20080924-ipc.shtml>

Revision 1.1

Last Updated 2009 April 16 2100 UTC (GMT)

For Public Release 2008 September 24 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 10000, uBR10012 and uBR7200 series devices use a User Datagram Protocol (UDP) based Inter-Process Communication (IPC) channel that is externally reachable. An attacker could exploit this

vulnerability to cause a denial of service (DoS) condition on affected devices. No other platforms are affected.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ipc.shtml>.

Note: The September 24, 2008 IOS Advisory bundled publication includes twelve Security Advisories. Eleven of the advisories address vulnerabilities in Cisco's IOS software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each Advisory lists the releases that correct the vulnerability described in the Advisory.

Individual publication links are listed below:

- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosips.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ssl.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-cucm.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-mfi.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ubr.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sccp.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosfw.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20080924-l2tp.shtml>

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

☐ Affected Products

Cisco 10000, uBR10012 and uBR7200 series devices that are running an affected version of Cisco IOS are affected.

☐ Vulnerable Products

Devices that are running Cisco IOS can be identified by using the **show version** command. The following example shows an output taken from a Cisco 10000 series device running Cisco IOS software release 12.2(31)SB10e:

```
c10k#show version | include IOS
Cisco IOS Software, 10000 Software (C10K3-P11-M), Version 12.2(31)SB10e,
c10k#
```

The following example shows an output taken from a Cisco uBR10012 series device running Cisco IOS software release 12.3(17b)BC7:

```
ubr10k#show version | include IOS
IOS (tm) 10000 Software (UBR10K-K8P6U2-M), Version 12.3(17b)BC7, RELEASE
ubr10k#
```

The following example shows an output taken from a Cisco uBR7200 series device running Cisco IOS software release 12.3(21a)BC2:

```
ubr7200#show version | include IOS
IOS (tm) 7200 Software (UBR7200-IK9SU2-M), Version 12.3(21a)BC2, RELEASE
ubr7200#
```

Please refer to the document entitled "White Paper: Cisco IOS Reference Guide" for additional information on the Cisco IOS release naming conventions. This document is available at the following link: <http://www.cisco.com/warp/public/620/1.html>

Any version of Cisco IOS prior to the fixed versions listed in the Software Versions and Fixes section below is vulnerable.

▣ Products Confirmed Not Vulnerable

Cisco uBR7100 series devices are not affected.

No other Cisco products are currently known to be affected by this vulnerability.

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

▣ Details

Cisco 10000, uBR10012 and uBR7200 series devices use a UDP-based IPC channel. This channel uses addresses from the 127.0.0.0/8 range and UDP port 1975. Cisco 10000, uBR10012 and uBR7200 series devices that are running an affected version of Cisco IOS will process IPC messages that are sent to UDP port 1975 from outside of the device. This behavior may be exploited by an attacker to cause a reload of the device, linecards, or both, resulting in a DoS condition.

Filtering unauthorized traffic destined to 127.0.0.0/8 or UDP port 1975 will mitigate this vulnerability.

This vulnerability is documented in the Cisco Bug IDs [CSCsg15342](#) ([registered](#) customers only) and [CSCsh29217](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2008-3805.

[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> .

CSCsg15342 - IPC processing needs to be more robust					
Calculate the environmental score of CSCsg15342					
CVSS Base Score - 8.5					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	Partial	Complete
CVSS Temporal Score - 7					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCsh29217 - IPC processing needs to be more robust					
Calculate the environmental score of CSCsh29217					
CVSS Base Score - 8.5					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	Partial	Complete
CVSS Temporal Score - 7					
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 reload of the device, linecards, or both, resulting in a DoS condition.

[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.

Each row of the Cisco IOS software table (below) names a Cisco IOS release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (along with the anticipated date of availability for each, if applicable) are listed in the "First Fixed Release" column of the table. The "Recommended Release" column indicates the releases which have fixes for all the published vulnerabilities at the time of this Advisory. 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. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Releases" column of the table.

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	Recommended Release
12.0	Not Vulnerable	
12.0DA	Not Vulnerable	
12.0DB	Not Vulnerable	
12.0DC	Not Vulnerable	
12.0S	Releases prior to 12.0(32)S are vulnerable, release 12.0(32)S and later are not vulnerable;	12.0(32)S11 12.0(33)S1
12.0SC	Not Vulnerable	
12.0SL	Vulnerable, migrate to 12.0S, 12.1	
12.0SP	Not Vulnerable	
12.0ST	Vulnerable, migrate to 12.0S, 12.1	
12.0SX	Not Vulnerable	
12.0SY	Not Vulnerable	
12.0SZ	12.0(30)SZ4	12.0(32)S11 12.0(33)S1

12.0T	Not Vulnerable	
12.0W	Not Vulnerable	
12.0WC	Not Vulnerable	
12.0WT	Not Vulnerable	
12.0XA	Not Vulnerable	
12.0XB	Not Vulnerable	
12.0XC	Not Vulnerable	
12.0XD	Not Vulnerable	
12.0XE	Not Vulnerable	
12.0XF	Not Vulnerable	
12.0XG	Not Vulnerable	
12.0XH	Not Vulnerable	
12.0XI	Not Vulnerable	
12.0XJ	Not Vulnerable	
12.0XK	Not Vulnerable	
12.0XL	Not Vulnerable	
12.0XM	Not Vulnerable	
12.0XN	Not Vulnerable	
12.0XQ	Not Vulnerable	
12.0XR	Not Vulnerable	
12.0XS	Not Vulnerable	
12.0XT	Not Vulnerable	
12.0XV	Not Vulnerable	
Affected 12.1-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.1 based releases		
Affected 12.2-Based Releases	First Fixed Release	Recommended Release
12.2	Not Vulnerable	
12.2B	Not Vulnerable	
12.2BC	Not Vulnerable	
12.2BW	Not Vulnerable	
12.2BX	Not Vulnerable	

12.2BY	Not Vulnerable	
12.2BZ	Not Vulnerable	
12.2CX	Not Vulnerable	
12.2CY	Not Vulnerable	
12.2CZ	Not Vulnerable	
12.2DA	Not Vulnerable	
12.2DD	Not Vulnerable	
12.2DX	Not Vulnerable	
12.2EW	Not Vulnerable	
12.2EWA	Not Vulnerable	
12.2EX	Not Vulnerable	
12.2EY	Not Vulnerable	
12.2EZ	Not Vulnerable	
12.2FX	Not Vulnerable	
12.2FY	Not Vulnerable	
12.2FZ	Not Vulnerable	
12.2IRB	Not Vulnerable	
12.2IXA	Not Vulnerable	
12.2IXB	Not Vulnerable	
12.2IXC	Not Vulnerable	
12.2IXD	Not Vulnerable	
12.2IXE	Not Vulnerable	
12.2IXF	Not Vulnerable	
12.2IXG	Not Vulnerable	
12.2JA	Not Vulnerable	
12.2JK	Not Vulnerable	
12.2MB	Not Vulnerable	
12.2MC	Not Vulnerable	
12.2S	Not Vulnerable	
12.2SB	12.2(31)SB13 12.2(33)SB1	12.2(33)SB2; Available on 26- SEP-08
12.2SBC	Not Vulnerable	
12.2SCA	12.2(33)SCA1	12.2(33)SCA1

12.2SE	Not Vulnerable	
12.2SEA	Not Vulnerable	
12.2SEB	Not Vulnerable	
12.2SEC	Not Vulnerable	
12.2SED	Not Vulnerable	
12.2SEE	Not Vulnerable	
12.2SEF	Not Vulnerable	
12.2SEG	Not Vulnerable	
12.2SG	Not Vulnerable	
12.2SGA	Not Vulnerable	
12.2SL	Not Vulnerable	
12.2SM	Not Vulnerable	
12.2SO	Not Vulnerable	
12.2SRA	Not Vulnerable	
12.2SRB	Not Vulnerable	
12.2SRC	12.2(33)SRC2	12.2(33)SRC2
12.2SU	Not Vulnerable	
12.2SV	Not Vulnerable	
12.2SVA	Not Vulnerable	
12.2SVC	Not Vulnerable	
12.2SVD	Not Vulnerable	
12.2SW	Not Vulnerable	
12.2SX	Not Vulnerable	
12.2SXA	Not Vulnerable	
12.2SXB	Not Vulnerable	
12.2SXD	Not Vulnerable	
12.2SXE	Not Vulnerable	
12.2SXF	Not Vulnerable	
12.2SXH	Not Vulnerable	
12.2SY	Not Vulnerable	
12.2SZ	Not Vulnerable	
12.2T	Not Vulnerable	
12.2TPC	Not Vulnerable	
12.2XA	Not Vulnerable	

12.2XB	Not Vulnerable	
12.2XC	Not Vulnerable	
12.2XD	Not Vulnerable	
12.2XE	Not Vulnerable	
12.2XF	Not Vulnerable	
12.2XG	Not Vulnerable	
12.2XH	Not Vulnerable	
12.2XI	Not Vulnerable	
12.2XJ	Not Vulnerable	
12.2XK	Not Vulnerable	
12.2XL	Not Vulnerable	
12.2XM	Not Vulnerable	
12.2XN	Not Vulnerable	
12.2XNA	Not Vulnerable	
12.2XNB	Not Vulnerable	
12.2XO	Not Vulnerable	
12.2XQ	Not Vulnerable	
12.2XR	Not Vulnerable	
12.2XS	Not Vulnerable	
12.2XT	Not Vulnerable	
12.2XU	Not Vulnerable	
12.2XV	Not Vulnerable	
12.2XW	Not Vulnerable	
12.2YA	Not Vulnerable	
12.2YB	Not Vulnerable	
12.2YC	Not Vulnerable	
12.2YD	Not Vulnerable	
12.2YE	Not Vulnerable	
12.2YF	Not Vulnerable	
12.2YG	Not Vulnerable	
12.2YH	Not Vulnerable	
12.2YJ	Not Vulnerable	
12.2YK	Not Vulnerable	
12.2YL	Not Vulnerable	

12.2YM	Not Vulnerable	
12.2YN	Not Vulnerable	
12.2YO	Not Vulnerable	
12.2YP	Not Vulnerable	
12.2YQ	Not Vulnerable	
12.2YR	Not Vulnerable	
12.2YS	Not Vulnerable	
12.2YT	Not Vulnerable	
12.2YU	Not Vulnerable	
12.2YV	Not Vulnerable	
12.2YW	Not Vulnerable	
12.2YX	Not Vulnerable	
12.2YY	Not Vulnerable	
12.2YZ	Not Vulnerable	
12.2ZA	Not Vulnerable	
12.2ZB	Not Vulnerable	
12.2ZC	Not Vulnerable	
12.2ZD	Not Vulnerable	
12.2ZE	Not Vulnerable	
12.2ZF	Not Vulnerable	
12.2ZG	Not Vulnerable	
12.2ZH	Not Vulnerable	
12.2ZJ	Not Vulnerable	
12.2ZL	Not Vulnerable	
12.2ZP	Not Vulnerable	
12.2ZU	Not Vulnerable	
12.2ZX	Vulnerable; first fixed in 12.2SB	12.2(33)SB2; Available on 26-SEP-08
12.2ZY	Not Vulnerable	
12.2ZYA	Not Vulnerable	
Affected 12.3-Based Releases	First Fixed Release	Recommended Release
12.3	Not Vulnerable	

12.3B	Not Vulnerable	
12.3BC	12.3(17b)BC6 12.3(21a)BC1 12.3(23)BC	12.3(23)BC4
12.3BW	Not Vulnerable	
12.3EU	Not Vulnerable	
12.3JA	Not Vulnerable	
12.3JEA	Not Vulnerable	
12.3JEB	Not Vulnerable	
12.3JEC	Not Vulnerable	
12.3JK	Not Vulnerable	
12.3JL	Not Vulnerable	
12.3JX	Not Vulnerable	
12.3T	Note: Releases prior to 12.3(14)T3 are vulnerable, release 12.3(14)T3 and later are not vulnerable;	12.4(15)T7 12.4(18c)
12.3TPC	Not Vulnerable	
12.3VA	Not Vulnerable	
12.3XA	Not Vulnerable	
12.3XB	Not Vulnerable	
12.3XC	Not Vulnerable	
12.3XD	Not Vulnerable	
12.3XE	Not Vulnerable	
12.3XF	Not Vulnerable	
12.3XG	Not Vulnerable	
12.3XI	12.3(7)XI10a	12.2(33)SB2; Available on 26-SEP-08
12.3XJ	Not Vulnerable	
12.3XK	Not Vulnerable	
12.3XL	Not Vulnerable	
12.3XQ	Not Vulnerable	
12.3XR	Not Vulnerable	

12.3XS	Not Vulnerable	
12.3XU	Not Vulnerable	
12.3XW	Not Vulnerable	
12.3XX	Not Vulnerable	
12.3XY	Not Vulnerable	
12.3XZ	Not Vulnerable	
12.3YA	Not Vulnerable	
12.3YD	Not Vulnerable	
12.3YF	Not Vulnerable	
12.3YG	Not Vulnerable	
12.3YH	Not Vulnerable	
12.3YI	Not Vulnerable	
12.3YJ	Not Vulnerable	
12.3YK	Not Vulnerable	
12.3YM	Not Vulnerable	
12.3YQ	Not Vulnerable	
12.3YS	Not Vulnerable	
12.3YT	Not Vulnerable	
12.3YU	Not Vulnerable	
12.3YX	Not Vulnerable	
12.3YZ	Not Vulnerable	
12.3ZA	Not Vulnerable	
Affected 12.4-Based Releases	First Fixed Release	Recommended Release
12.4	Note: Releases prior to 12.4(3) are vulnerable, release 12.4(3) and later are not vulnerable;	12.4(18c)
12.4JA	Not Vulnerable	
12.4JK	Not Vulnerable	
12.4JL	Not Vulnerable	
12.4JMA	Not Vulnerable	
12.4JMB	Not Vulnerable	
12.4JMC	Not Vulnerable	

12.4JX	Not Vulnerable	
12.4MD	Not Vulnerable	
12.4MR	Not Vulnerable	
12.4SW	Not Vulnerable	
12.4T	Not Vulnerable	
12.4XA	Not Vulnerable	
12.4XB	Not Vulnerable	
12.4XC	Not Vulnerable	
12.4XD	Not Vulnerable	
12.4XE	Not Vulnerable	
12.4XF	Not Vulnerable	
12.4XG	Not Vulnerable	
12.4XJ	Not Vulnerable	
12.4XK	Not Vulnerable	
12.4XL	Not Vulnerable	
12.4XM	Not Vulnerable	
12.4XN	Not Vulnerable	
12.4XP	Not Vulnerable	
12.4XQ	Not Vulnerable	
12.4XR	Not Vulnerable	
12.4XT	Not Vulnerable	
12.4XV	Not Vulnerable	
12.4XW	Not Vulnerable	
12.4XY	Not Vulnerable	
12.4XZ	Not Vulnerable	
12.4YA	Not Vulnerable	

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

☐ Workarounds

Workarounds consist of filtering packets that are sent to 127.0.0.0/8 range and UDP packets that are sent to port 1975.

Using Interface Access Control Lists

Access lists that filter UDP packets destined to port 1975 can be used to mitigate this vulnerability.

UDP port 1975 is a registered port number that can be used by certain applications. However, filtering all packets that are destined to UDP port 1975 may cause some applications to malfunction. Therefore, access lists need to explicitly deny UDP 1975 packets that are sent to any router interface IP addresses and permit transit traffic. Such access lists need to be applied on all interfaces to be effective. Since the IPC channel uses addresses from the 127.0.0.0/8 range, it is also necessary to filter packets that are sourced from or destined to this range. An example is given below:

```
access-list 100 deny udp any host <router-interface 1> eq 1975
access-list 100 deny udp any host <router-interface 2> eq 1975
access-list 100 deny udp any host <router-interface ...> eq 1975
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
access-list 100 deny ip any 127.0.0.0 0.255.255.255
access-list 100 permit ip any any

interface Serial 0/0
 ip access-group 100 in
```

Using Control Plane Policing

Control Plane Policing (CoPP) can be used to block untrusted UDP port 1975 access to the affected device. Cisco IOS software releases 12.2BC and 12.2SCA support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example can be adapted to your network.

Note: CoPP is not supported on uBR10012 series devices.

```
!-- Permit all UDP/1975 traffic so that it
!-- will be policed and dropped by the CoPP feature

!
access-list 111 permit udp any any eq 1975
access-list 111 permit ip any 127.0.0.0 0.255.255.255
access-list 111 permit ip 127.0.0.0 0.255.255.255 any
!

!-- Permit (Police or Drop)/Deny (Allow) all other Layer 3 and
!-- Layer 4 traffic in accordance with existing security policies
!-- and configurations for traffic that is authorized to be sent
!-- to infrastructure devices

!

!-- Create a Class-Map for traffic to be policed by the CoPP
!-- feature

!
class-map match-all drop-IPC-class
 match access-group 111
!

!-- Create a Policy-Map that will be applied to the Control-Plane
!-- of the device
```

```

!
policy-map drop-IPC-traffic
  class drop-IPC-class
    drop
!
!-- Apply the Policy-Map to the Control-Plane of the device
!
control-plane
  service-policy input drop-IPC-traffic
!

```

In the above CoPP example, the access control list entries (ACEs) which match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function.

Please note that in the Cisco IOS 12.2S and 12.0S trains the policy-map syntax is different:

```

!
policy-map drop-IPC-traffic class drop-IPC-class
  police 32000 1500 1500 conform-action drop exceed-action drop
!

```

Additional information on the configuration and use of the CoPP feature can be found at http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html, http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900, and http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/grtlimt.html.

Using Infrastructure ACLs at Network Boundary

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. iACLs are 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 iACL example shown below should be included as part of the deployed infrastructure access-list which will protect all devices with IP addresses in the infrastructure IP address range:

```

!-- Note: IPC packets sent to UDP destination port 1975 must not
!-- be permitted from any trusted source as this traffic
!-- should only be sent and received internally by the
!-- affected device using an IP address allocated from the
!-- 127.0.0.0/8 prefix.
!--
!-- IPC that traffic that is internally generated and sent
!-- and/or received by the affected device is not subjected
!-- to packet filtering by the applied iACL policy.
!
!-- Deny IPC (UDP port 1975) packets from all sources destined to
!-- all IP addresses configured on the affected device.

```

```

!
access-list 150 deny udp any host INTERFACE_ADDRESS#1 eq 1975
access-list 150 deny udp any host INTERFACE_ADDRESS#2 eq 1975
access-list 150 deny udp any host INTERFACE_ADDRESS#N eq 1975
!

!-- Deny all IP packets with a source or destination IP address
!-- from the 127.0.0.0/8 prefix.

!
access-list 150 deny ip 127.0.0.0 0.255.255.255 any
access-list 150 deny ip any 127.0.0.0 0.255.255.255
!

!-- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations.

!

!-- Permit all other traffic to transit the device.

!
access-list 150 permit ip any any
!

!-- Apply iACL to interfaces in the ingress direction.

!
interface GigabitEthernet0/0
 ip access-group 150 in
!

```

Note: iACLs that filter UDP packets destined to port 1975 can be used to mitigate this vulnerability. However, UDP port 1975 is a registered port number that can be used by certain applications. Filtering all packets that are destined to UDP port 1975 may cause some applications to malfunction. Therefore, the iACL policy needs to explicitly deny UDP packets using a destination port of 1975 that are sent to any router interface IP addresses for affected devices, then permit and/or deny all other Layer 3 and Layer 4 traffic in accordance with existing security policies and configurations, and then permit all other traffic to transit the device. iACLs must be applied on all interfaces to be used effectively. Since the IPC channel uses addresses from the 127.0.0.0/8 range, it is also necessary to filter packets that are sourced from or destined to this range as provided in the preceding example.

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained here:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

Additional Mitigation Techniques

Additional mitigation techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory, which is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-amb-20080924-ipc-and-ubr.shtml>

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

☐ **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 found internally.

[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-20080924-ipc.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-bulletins@lists.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 1.1	2009- April-16	Removed references to the combined software table, as it is now outdated
Revision 1.0	2008- Sep-24	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>.

[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.](#)