

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

Cisco Security Advisory: Multiple Multicast Vulnerabilities in Cisco IOS Software

Advisory ID: cisco-sa-20080924-multicast

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

Revision 1.3

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

Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

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

☐ Vulnerable Products

Devices that are running Cisco IOS Software and configured for PIM have a vulnerability related to a specially crafted PIM packet. In addition, Cisco 12000 Series (GSR) routers running Cisco IOS Software have a second vulnerability related to a crafted multicast packet.

The **show running-config | include ip pim** command can be issued to verify that a Cisco IOS device is configured for PIM. In the following example, the Cisco IOS router is configured for PIM sparse-dense mode.

```
Router#show running-config | include ip pim
ip pim sparse-dense-mode
```

Note that available PIM modes on a Cisco IOS device are dense mode, sparse mode, or sparse-dense mode. A device that is configured for any of these modes is affected by these vulnerabilities. The mode determines how the device populates its multicast routing table and how multicast packets are forwarded. PIM must be enabled in one of these modes on at least one interface in order for a device to process IP multicast routing. There is no default mode setting. Multicast routing is disabled by default. However, a Cisco IOS device is vulnerable if at least one interface is configured for PIM.

Additionally, To display information about interfaces configured for Protocol Independent Multicast (PIM), use the **show ip pim interface** command in user EXEC or privileged EXEC mode, as shown in the following example:

```
Router# show ip pim interface
```

Address	Interface	Ver/ Mode	Nbr Count	Query Intvl	DR Prior	DR
10.1.0.1	GigabitEthernet0/0	v2/SD	0	30	1	10.
10.6.0.1	GigabitEthernet0/1	v2/SD	1	30	1	10.

In order to determine the software that runs on a Cisco IOS product, log in to the device and issue the show version command to display the system banner. Cisco IOS software identifies itself as "Internetwork Operating System Software" or simply "IOS." On the next line of output, the image name displays between parentheses, followed by "Version" and the Cisco IOS release name. Other Cisco devices do not have the show version command or give different output.

The following example shows output from a device that runs an IOS image:

```
router>show version
Cisco IOS Software, 7200 Software (C7200-ADVSECURITYK9-M), Version 12.4(6
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 16-May-06 16:09 by kellythw
<more output removed for brevity>
```

▣ Products Confirmed Not Vulnerable

Cisco IOS devices that are not configured for PIM are not vulnerable. Cisco IOS XR Software is not affected by this vulnerability. No other Cisco products are currently known to be affected by this vulnerability.

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

▣ Details

Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS Software that may lead to a denial of service (DoS) condition. Devices that run Cisco IOS Software and are configured for PIM are affected by the first vulnerability. Only Cisco 12000 Series (GSR) routers that are configured for PIM are affected by the second vulnerability.

Available PIM modes on a Cisco IOS device are dense mode, sparse mode, or sparse-dense mode. The mode determines how the device populates its multicast routing table and how multicast packets are forwarded. PIM must be enabled in one of these modes on at least one interface in order for a device to process IP multicast routing.

Note: There is no default mode setting. Multicast routing is disabled by default. However, a Cisco IOS device is vulnerable if at least one interface is configured for PIM.

To configure PIM on an interface to be in dense mode, use the following command in interface configuration mode:

```
Router(config-if)# ip pim dense-mode
```

To configure PIM on an interface to be in sparse mode, use the following command in interface configuration mode:

```
Router(config-if)# ip pim sparse-mode
```

To configure PIM on an interface to be in sparse-dense mode, use the following command in interface configuration mode:

```
Router(config-if)# ip pim sparse-dense-mode
```

These vulnerabilities are documented in the following Cisco Bug IDs:

- CSCsd95616 - Crafted PIM packets may cause an IOS device to reload
- CSCsl34355 - GSR may crash when processing a malformed multicast packet

These vulnerabilities have been assigned the Common Vulnerabilities and Exposures (CVE) identifiers CVE-2008-3808 and CVE-2008-3809.

[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>.

CSCsd95616 - Crafted PIM packets may cause an IOS device to reload					
Calculate the environmental score of CSCsd95616					
CVSS Base Score - 7.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact

Network	Low	None	None	None	Complete
CVSS Temporal Score - 6.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCs134355 - GSR may crash when processing a malformed multicast packet					
Calculate the environmental score of CSCs134355					
CVSS Base Score - 7.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	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 may cause a reload of the affected device. Repeated exploitation could result in a sustained denial of service (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	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0DA	Releases prior to 12.0(8)DA3 are vulnerable, release 12.0(8)DA3 and later are not vulnerable; first fixed in 12.2DA	12.2(12)DA13 12.4(15)T7 12.4(18c)
12.0DB	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0DC	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0S	12.0(32)S8 12.0(33)S	12.0(32)S11 12.0(33)S1
12.0SC	Vulnerable; first fixed in 12.0S	12.0(32)S11 12.0(33)S1
12.0SL	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0SP	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0ST	Vulnerable; first fixed in 12.0S	12.0(32)S11 12.0(33)S1
12.0SX	Vulnerable; first fixed in 12.0S	12.0(32)S11 12.0(33)S1
12.0SY	12.0(32)SY5	12.0(32)SY7; Available on 29-SEP-08
		12.0(32)S11

12.0SZ	12.0(30)SZ4	12.0(33)S1
12.0T	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0W	Vulnerable; first fixed in 12.2	12.0(3c)W5(8)
12.0WC	Releases prior to 12.0(5)WC10 are vulnerable, release 12.0(5)WC10 and later are not vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0WT	Not Vulnerable	
12.0XA	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XB	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XC	Releases prior to 12.0(2)XC2 are vulnerable, release 12.0(2)XC2 and later are not vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XD	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XE	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XF	Not Vulnerable	
12.0XG	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XH	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XI	Releases prior to 12.0(4)XI2 are vulnerable, release 12.0(4)XI2 and later are not vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)

12.0XJ	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XK	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XL	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XM	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XN	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XQ	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XR	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XS	Not Vulnerable	
12.0XT	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XV	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
Affected 12.1-Based Releases	First Fixed Release	Recommended Release
12.1	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1AA	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1AX	Vulnerable; first fixed in 12.2EY	12.2(46)SE
12.1AY	Releases prior to 12.1(22)AY1 are vulnerable, release 12.1(22)AY1	12.1(22)EA12

	and later are not vulnerable; first fixed in 12.1EA	12.2(46)SE
12.1AZ	Not Vulnerable	
12.1CX	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1DA	Vulnerable; first fixed in 12.2DA	12.2(12)DA13 12.4(15)T7 12.4(18c)
12.1DB	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1DC	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1E	12.1(27b)E2	12.2(18)SXF15
12.1EA	12.1(22)EA10	12.1(22)EA12
12.1EB	Vulnerable; contact TAC	
12.1EC	Vulnerable; first fixed in 12.3BC	12.2(33)SCA1 12.3(23)BC4
12.1EO	Vulnerable; first fixed in 12.2SV	
12.1EU	Vulnerable; first fixed in 12.2EWA	12.2(25)EWA14 12.2(31)SGA8 12.2(46)SG1
12.1EV	Not Vulnerable	
12.1EW	Vulnerable; first fixed in 12.2	12.2(25)EWA14 12.2(31)SGA8 12.2(46)SG1 12.4(15)T7 12.4(18c)

12.1EX	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1EY	Vulnerable; contact TAC	
12.1EZ	Vulnerable; first fixed in 12.1E	12.2(18)SXF15 12.4(15)T7 12.4(18c)
12.1GA	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1GB	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1T	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XA	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XB	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XC	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XD	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XE	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XF	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XG	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XH	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)

12.1XI	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XJ	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XL	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XM	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XP	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XQ	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XR	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XS	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XT	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XU	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XV	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XW	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XX	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XY	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)

12.1XZ	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1YA	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1YB	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1YC	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1YD	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1YE	Releases prior to 12.1(5)YE6 are vulnerable, release 12.1(5)YE6 and later are not vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1YF	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1YH	Vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1YI	Vulnerable; contact TAC	
12.1YJ	Not Vulnerable	
Affected 12.2-Based Releases	First Fixed Release	Recommended Release
12.2	12.2(26c) 12.2(27c) 12.2(28d) 12.2(29b) 12.2(46)	12.4(15)T7 12.4(18c)
12.2B	Vulnerable; first fixed in 12.3	12.4(15)T7

		12.4(18c)
12.2BC	Vulnerable; first fixed in 12.3	12.2(33)SCA1 12.3(23)BC4 12.4(15)T7 12.4(18c)
12.2BW	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2BX	Vulnerable; first fixed in 12.3	12.2(33)SB2; Available on 26-SEP-08 12.4(15)T7 12.4(18c)
12.2BY	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2BZ	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2CX	Vulnerable; first fixed in 12.3	12.2(33)SCA1 12.3(23)BC4 12.4(15)T7 12.4(18c)
12.2CY	Vulnerable; first fixed in 12.3	12.2(33)SCA1 12.3(23)BC4 12.4(15)T7 12.4(18c)
12.2CZ	Vulnerable; first fixed in 12.2S	12.2(33)SB2; Available on 26-SEP-08
12.2DA	12.2(10)DA9 12.2(12)DA13	12.2(12)DA13

12.2DD	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2DX	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2EW	Vulnerable; first fixed in 12.2EWA	12.2(25)EWA14 12.2(31)SGA8 12.2(46)SG1
12.2EWA	12.2(25)EWA10 12.2(25)EWA11	12.2(25)EWA14
12.2EX	12.2(37)EX	12.2(35)EX2
12.2EY	12.2(37)EY	
12.2EZ	Vulnerable; first fixed in 12.2SEE	12.2(46)SE
12.2FX	Not Vulnerable	
12.2FY	Not Vulnerable	
12.2FZ	Vulnerable; first fixed in 12.2SE	12.2(46)SE
12.2IRB	Not Vulnerable	
12.2IXA	Vulnerable; migrate to any release in 12.2IXE	12.2(18)IXG
12.2IXB	Vulnerable; migrate to any release in 12.2IXE	12.2(18)IXG
12.2IXC	Vulnerable; migrate to any release in 12.2IXE	12.2(18)IXG
12.2IXD	Vulnerable; migrate to any release in 12.2IXE	12.2(18)IXG
12.2IXE	Not Vulnerable	
12.2IXF	Not Vulnerable	
12.2IXG	Not Vulnerable	
12.2JA	Not Vulnerable	
12.2JK	Not Vulnerable	
12.2MB	Vulnerable; first fixed in 12.2SW	12.2(25)SW12 12.4(15)T7

		12.4(18c)
12.2MC	12.2(15)MC2i	12.4(15)T7 12.4(18c)
12.2S	12.2(14)S18 12.2(18)S13 12.2(20)S13 12.2(25)S13	12.2(33)SB2; Available on 26- SEP-08
12.2SB	12.2(28)SB7 12.2(31)SB5 12.2(33)SB	12.2(33)SB2; Available on 26- SEP-08
12.2SBC	Vulnerable; first fixed in 12.2SB	12.2(33)SB2; Available on 26- SEP-08
12.2SCA	Not Vulnerable	
12.2SE	12.2(35)SE4 12.2(37)SE	12.2(46)SE
12.2SEA	Vulnerable; first fixed in 12.2SEE	12.2(46)SE
12.2SEB	Vulnerable; first fixed in 12.2SEE	12.2(46)SE
12.2SEC	Vulnerable; first fixed in 12.2SEE	12.2(46)SE
12.2SED	Vulnerable; first fixed in 12.2SEE	12.2(46)SE
12.2SEE	12.2(25)SEE4	12.2(46)SE
12.2SEF	Not Vulnerable	
12.2SEG	12.2(25)SEG3	12.2(25)SEG6
12.2SG	12.2(25)SG3 12.2(31)SG3 12.2(37)SG	12.2(46)SG1
12.2SGA	12.2(31)SGA2	12.2(31)SGA8
12.2SL	Not Vulnerable	

12.2SM	12.2(29)SM3	12.2(29)SM4
12.2SO	Vulnerable; first fixed in 12.2SV	
12.2SRA	12.2(33)SRA4	12.2(33)SRB4 12.2(33)SRC2
12.2SRB	Not Vulnerable	
12.2SRC	Not Vulnerable	
12.2SU	Vulnerable; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.2SV	12.2(29b)SV1	
12.2SVA	Not Vulnerable	
12.2SVC	Not Vulnerable	
12.2SVD	Not Vulnerable	
12.2SW	12.2(25)SW12	12.2(25)SW12
12.2SX	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF15
12.2SXA	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF15
12.2SXB	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF15
12.2SXD	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF15
12.2SXE	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF15
12.2SXF	12.2(18)SXF9	12.2(18)SXF15
12.2SXH	Not Vulnerable	
12.2SY	Vulnerable; first fixed in 12.2S	12.2(33)SB2; Available on 26-SEP-08
12.2SZ	Vulnerable; first fixed in 12.2S	12.2(33)SB2; Available on 26-SEP-08
12.2T	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2TPC	Vulnerable; contact TAC	

12.2XA	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XB	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XC	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XD	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XE	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XF	Vulnerable; first fixed in 12.3	12.2(33)SCA1 12.3(23)BC4 12.4(15)T7 12.4(18c)
12.2XG	Releases prior to 12.2(2)XG1 are vulnerable, release 12.2(2)XG1 and later are not vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XH	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XI	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XJ	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XK	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XL	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
	Vulnerable; first fixed	12.4(15)T7

12.2XM	in 12.3	12.4(18c)
12.2XN	12.2(33)XN1	12.2(33)SB2; Available on 26-SEP-08 12.2(33)SRC2 12.2(33)XNA2
12.2XNA	Not Vulnerable	
12.2XNB	Not Vulnerable	
12.2XO	Not Vulnerable	
12.2XQ	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XR	Releases prior to 12.2(15)XR are vulnerable, release 12.2(15)XR and later are not vulnerable; first fixed in 12.3	12.3(8)JEA3 12.4(15)T7 12.4(18c)
12.2XS	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XT	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XU	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XV	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XW	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2YA	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2YB	Vulnerable; contact TAC	
12.2YC	Vulnerable; contact TAC	
	Vulnerable; contact	

12.2YD	TAC	
12.2YE	Vulnerable; contact TAC	
12.2YF	Vulnerable; contact TAC	
12.2YG	Vulnerable; contact TAC	
12.2YH	Vulnerable; contact TAC	
12.2YJ	Vulnerable; contact TAC	
12.2YK	Vulnerable; contact TAC	
12.2YL	Vulnerable; contact TAC	
12.2YM	Vulnerable; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.2YN	Vulnerable; contact TAC	
12.2YO	Vulnerable; contact TAC	
12.2YP	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2YQ	Vulnerable; contact TAC	
12.2YR	Vulnerable; contact TAC	
12.2YS	Not Vulnerable	
12.2YT	Vulnerable; contact TAC	
12.2YU	Vulnerable; contact TAC	
12.2YV	Vulnerable; contact TAC	
12.2YW	Vulnerable; contact TAC	
12.2YX	Vulnerable; contact TAC	

12.2YY	Vulnerable; contact TAC	
12.2YZ	Vulnerable; contact TAC	
12.2ZA	Vulnerable; first fixed in 12.2SXF	12.2(18)SXF15
12.2ZB	Vulnerable; contact TAC	
12.2ZC	Vulnerable; contact TAC	
12.2ZD	Vulnerable; contact TAC	
12.2ZE	Vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2ZF	Vulnerable; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.2ZG	Vulnerable; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.2ZH	12.2(13)ZH9	12.4(15)T7 12.4(18c)
12.2ZJ	Vulnerable; contact TAC	
12.2ZL	Vulnerable; contact TAC	
12.2ZP	Vulnerable; contact TAC	
12.2ZU	Vulnerable; migrate to any release in 12.2SXH	12.2(33)SXH3
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(17c)	

12.3	12.3(18a)	
	12.3(19a)	12.4(15)T7
	12.3(20a)	12.4(18c)
	12.3(21)	
12.3B	Vulnerable; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3BC	12.3(17b)BC6 12.3(21)BC	12.3(23)BC4
12.3BW	Vulnerable; first fixed in 12.4	12.4(15)T7 12.4(18c)
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	Vulnerable; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3TPC	Vulnerable; contact TAC	
12.3VA	Not Vulnerable	
12.3XA	12.3(2)XA7	12.4(15)T7 12.4(18c)
12.3XB	Vulnerable; contact TAC	
12.3XC	Vulnerable; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3XD	Vulnerable; first fixed in 12.4	12.4(15)T7

		12.4(18c)
12.3XE	Vulnerable; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3XF	Vulnerable; contact TAC	
12.3XG	Vulnerable; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3XI	12.3(7)XI10	12.2(33)SB2; Available on 26-SEP-08
12.3XJ	Vulnerable; first fixed in 12.3YX	12.3(14)YX13 12.4(15)T7
12.3XK	Vulnerable; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3XL	Vulnerable; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3XQ	Vulnerable; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3XR	12.3(7)XR7	12.4(15)T7 12.4(18c)
12.3XS	Vulnerable; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3XU	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.3XW	Vulnerable; first fixed in 12.3YX	12.3(14)YX13 12.4(15)T7
12.3XX	12.3(8)XX2d	12.4(15)T7 12.4(18c)
12.3XY	Vulnerable; first fixed in 12.4	12.4(15)T7 12.4(18c)
		12.4(15)T7

12.3XZ	Vulnerable; first fixed in 12.4	12.4(18c)
12.3YA	Vulnerable; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3YD	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.3YF	Vulnerable; first fixed in 12.3YX	12.3(14)YX13 12.4(15)T7
12.3YG	12.3(8)YG6	12.4(15)T7
12.3YH	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.3YI	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.3YJ	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.3YK	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.3YM	12.3(14)YM10	12.3(14)YM13; Available on 30-SEP-08
12.3YQ	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.3YS	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.3YT	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.3YU	Vulnerable; first fixed in 12.4XB	12.4(2)XB10 12.4(9)XG3 12.4(15)T7
12.3YX	12.3(14)YX8	12.3(14)YX13
12.3YZ	12.3(11)YZ3	
12.3ZA	Vulnerable; first fixed in 12.4T	12.4(15)T7
Affected 12.4-Based Releases	First Fixed Release	Recommended Release
	12.4(10c)	

12.4	12.4(12) 12.4(3h) 12.4(5c) 12.4(7e) 12.4(8d)	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	12.4(11)MR	12.4(19)MR
12.4SW	Not Vulnerable	
12.4T	12.4(11)T 12.4(2)T6 12.4(4)T8 12.4(6)T7 12.4(9)T3	12.4(15)T7
12.4XA	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.4XB	12.4(2)XB6	12.4(2)XB10
12.4XC	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.4XD	12.4(4)XD8	12.4(4)XD11; Available on 26-SEP-08
12.4XE	Vulnerable; first fixed in 12.4T	12.4(15)T7
12.4XF	Not Vulnerable	
12.4XG	12.4(9)XG2	12.4(9)XG3

12.4XJ	Not Vulnerable	
12.4XK	Not Vulnerable	
12.4XL	Not Vulnerable	
12.4XM	Not Vulnerable	
12.4XN	Not Vulnerable	
12.4XP	Vulnerable; contact TAC	
12.4XQ	Not Vulnerable	
12.4XR	Not Vulnerable	
12.4XT	12.4(6)XT2	12.4(15)T7
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

There are no workarounds for the second vulnerability. The following workarounds only apply to the vulnerability addressed in Cisco bug ID CSCsd95616. A PIM router must receive PIM Hellos to establish PIM neighborship. PIM neighborship is also the basis for designated router (DR) election, DR failover, and accepting/sending PIM Join/Prune/Assert messages. To specify trusted PIM neighbors, use the **ip pim neighbor-filter** command, as shown in the following example:

```
Router(config)#access-list 1 permit host 10.10.10.123

!-- An access control list is created to allow a trusted PIM neighbor
!-- in this example the neighbor is 10.10.10.123
!

Router(config)#interface fastEthernet 0/0
Router(config-if)#ip pim neighbor-filter 1

!-- The PIM neighbor filter is then applied to the respective interface(s)
```

The **ip pim neighbor-filter** command filters PIM packets from untrusted devices including Hellos, Join/Prune, and BSR packets.

Note: The vulnerabilities described in this document can be exploited by spoofed IP packets if the attacker knows the IP address of the trusted PIM neighbors listed in the **ip pim neighbor-filter** implementation.

To protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, administrators are advised to deploy ACLs to perform policy enforcement of traffic sent to core infrastructure equipment. PIM is IP protocol 103. As an additional workaround, administrators can explicitly permit only authorized PIM (IP protocol 103) traffic sent to infrastructure devices in accordance with existing security policies and configurations. An ACL can be deployed as shown in the following example:

```
ip access-list extended Infrastructure-ACL-Policy

!
!-- When applicable, include explicit permit statements for trusted
!-- sources that require access on the vulnerable protocol
!-- PIM routers need to communicate with the rendezvous point (RP).
!-- In this example, 192.168.100.1 is the IP address of the
!-- rendezvous point, which is a trusted host that requires access
!-- to and from the affected PIM devices.
!

permit pim host 192.168.100.1 192.168.60.0 0.0.0.255
permit pim 192.168.60.0 0.0.0.255 host 192.168.100.1

!
!-- Permit PIM segment traffic, packets have destination of:
!-- 224.0.0.13 (PIMv2)
!-- 224.0.0.2 (Required only by legacy PIMv1)
!

permit pim 192.168.60.0 0.0.0.255 host 224.0.0.13
permit pim 192.168.60.0 0.0.0.255 host 224.0.0.2

!
!-- The following vulnerability-specific access control entries
!-- (ACEs) can aid in identification of attacks
!

deny pim any 192.168.60.0 0.0.0.255

!
!-- Explicit deny ACE for traffic sent to addresses configured within
!-- the infrastructure address space
!

deny ip any 192.168.60.0 0.0.0.255

!
!-- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations
!
!-- Apply iACL to interfaces in the ingress direction
!

interface GigabitEthernet0/0
 ip access-group Infrastructure-ACL-Policy in
```

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory:

<http://www.cisco.com/warp/public/707/cisco-amb-20080924-multicast.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 vulnerabilities described in this advisory.

These vulnerabilities were found during internal testing.

[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-multicast.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 1.3	2009-April-16	Removed references to the combined software table, as it is now outdated.
Revision 1.2	2008-October-14	Workaround information update.
Revision 1.1	2008-September-27	Clarify that a Cisco IOS device is vulnerable if at least one interface is configured for PIM.
Revision 1.0	2008-September-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.](#)