

Table of Contents

<u>Cisco Security Advisory: Cisco IOS Interface Blocked by IPv4 Packets</u>	1
<u>Revision 1.15</u>	1
<u>Last Updated 2004 July 22 at 20:00 UTC (GMT)</u>	1
<u>For Public Release 2003 July 16 at 6:10 UTC (GMT)</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Affected Products</u>	1
<u>Details</u>	2
<u>Impact</u>	3
<u>Software Versions and Fixes</u>	3
<u>Cisco IOS Software</u>	3
<u>Cisco ONS 15454 Software</u>	12
<u>Obtaining Fixed Software</u>	12
<u>Workarounds</u>	12
<u>Exploitation and Public Announcements</u>	14
<u>Status of This Notice: INTERIM</u>	14
<u>Distribution</u>	14
<u>Revision History</u>	15
<u>Cisco Security Procedures</u>	16

Cisco Security Advisory: Cisco IOS Interface Blocked by IPv4 Packets

Revision 1.15

Last Updated 2004 July 22 at 20:00 UTC (GMT)

For Public Release 2003 July 16 at 6:10 UTC (GMT)

Please provide your feedback on this document.

Summary
Affected Products
Details
Impact
Software Versions and Fixes
Obtaining Fixed Software
Workarounds
Exploitation and Public Announcements
Status of This Notice: INTERIM
Distribution
Revision History
Cisco Security Procedures

Summary

Cisco routers and switches running Cisco IOS[®] software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. Multiple IPv4 packets with specific protocol fields sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. Traffic passing through the device cannot block the input queue. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. Multiple valid workarounds are available in the form of best practices for situations where software upgrades are not currently feasible.

Cisco has made software available, free of charge, to correct the problem.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml>.

Affected Products

This issue affects all Cisco devices running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets. This includes routers as well as switches and line cards which run Cisco IOS software. Cisco devices which do not run Cisco IOS software are not affected. Devices which run only Internet Protocol version 6 (IPv6) are not affected.

To determine the software running on a Cisco 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 IOS release name. Other Cisco devices will not have the **show version** command or will give different output.

The following example identifies a Cisco product running IOS release 12.0(3) with an installed image name of C2500-IS-L:

```
Cisco Internetwork Operating System Software IOS (TM)
2500 Software (C2500-IS-L), Version 12.0(3), RELEASE SOFTWARE
```

The release train label is "12.0".

The next example shows a product running IOS release 12.0(2a)T1 with an image name of C2600-JS-MZ:

```
Cisco Internetwork Operating System Software IOS (tm)
C2600 Software (C2600-JS-MZ), Version 12.0(2a)T1, RELEASE SOFTWARE (fc1)
```

Additional information about Cisco IOS Banners is available at http://www.cisco.com/en/US/products/sw/iosswrel/ios_abcs_ios_networking_the_enterprise0900aecd800a4e15.html.

The Cisco ONS 15454 ML-Series cards use the Cisco IOS Software to deliver Layer 2 and Layer 3 functionality and are provisioned via the Cisco IOS Software command-line interface. Cisco ONS 15454 Software Release 4.0.0 is vulnerable except when the ML-Series interfaces are in Bridge-only mode. Only the ML-Series cards are affected, the ONS 15454 controller processor (TCC/TCC+/TCC2) does not run IOS and therefore is not affected by this vulnerability.

Details

Cisco routers are configured to process and accept Internet Protocol version 4 (IPv4) packets by default. IPv4 packets handled by the processor on a Cisco IOS device with protocol types of 53 (SWIPE), 55 (IP Mobility, or 77 (Sun ND), all with Time-to-Live (TTL) values of 1 or 0, and 103 (Protocol Independent Multicast – PIM) with any TTL value, may force the device to incorrectly flag the input queue on an interface as full. A full input queue will stop the device from processing inbound traffic on that interface and may result in routing protocols dropping due to dead timers.

Routers that have the PIM process running are not affected by traffic with protocol type 103. This process will be created when PIM is configured on any interface of the router. An interface with PIM enabled will have one of the following three commands in the interface configuration: **ip pim dense-mode**, **ip pim sparse-mode**, or **ip pim sparse-dense-mode**. Devices with input queues blocked with only PIM packets may have additional workaround options, which are listed in the Workarounds section.

On a blocked Ethernet interface, Address Resolution Protocol (ARP) times out after a default time of four hours, and no traffic can be processed. The device must be rebooted to clear the input queue on the interface, and will not reload without user intervention. The attack may be repeated on all interfaces causing the router to be remotely inaccessible. A workaround is available, and is documented in the Workarounds section. Other types of interfaces, including but not limited to ATM, Serial and POS interfaces, may still be affected, but ARP is no longer a factor.

The Cisco vulnerabilities are documented in the following two bug IDs: CSCea02355 (registered customers only) affects all Cisco routers running Cisco IOS software, documents the flaw with protocols 53, 55, and 77, and was introduced with bug ID CSCdi22941 (registered customers only) . CSCdz71127 (registered customers only) was introduced by an earlier code revision, and documents an input queue vulnerability to protocol 103 with a

Cisco Security Advisory: Cisco IOS Interface Blocked by IPv4 Packets

device which is not configured for PIM. Any version of software which has the fix for CSCdx02283 (registered customers only) is vulnerable.

To identify a blocked input interface, use the **show interfaces** command and look for the Input Queue line. If the current size (in this case, 76) is larger than the maximum size (75), the input queue is blocked.

Use the **show buffers** command and look for the prot field. Below are two examples:

```
Router#show interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is 0050.500e.f1e0 (bia 0050.500e.f1e0)
  Internet address is 172.16.1.9/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:41, output 00:00:07, output hang never
  Last clearing of "show interface" counters 00:07:18
  Input queue: 76/75/1091/0 (size/max/drops/flushes); Total output drops: 0
  !--- The 76/75 shows that this is blocked
```

```
Router#show buffers input-interface serial 0/0 packet
Buffer information for Small buffer at 0x612EAF3C
data_area 0x7896E84, refcount 1, next 0x0, flags 0x0
linktype 7 (IP), enctype 0 (None), encsize 46, rxttype 0
if_input 0x6159D340 (FastEthernet3/2), if_output 0x0 (None)
inputtime 0x0, outputtime 0x0, oqnumber 65535
datagramstart 0x7896ED8, datagramsize 728, maximum size 65436
mac_start 0x7896ED8, addr_start 0x7896ED8, info_start 0x0
network_start 0x7896ED8, transport_start 0x0
source: 10.0.0.1, destination: 192.168.10.10, id: 0xAAB8, ttl: 41, prot: 103
  !--- prot: 103 is proof that this is one of the attack packets
```

Impact

A device receiving these specifically crafted IPv4 packets will force the inbound interface to stop processing traffic. The device may stop processing packets destined to the router, including routing protocol packets and ARP packets. No alarms will be triggered, nor will the router reload to correct itself. This issue can affect all Cisco devices running Cisco IOS software. This vulnerability may be exercised repeatedly resulting in loss of availability until a workaround has been applied or the device has been upgraded to a fixed version of code.

In addition to the command-line instructions to definitively show impacted interfaces, the white paper entitled "Uses of Network Management for Monitoring of the "IP Packet Blocks Input Queue" PSIRT Advisory" details methods to identify impacted devices via SNMP, RMON, and Network Management products.

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

Software Versions and Fixes

Cisco IOS Software

Each row of the table 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 and the anticipated date of

availability for each are listed in the Rebuild, Interim, and Maintenance columns. In some cases, no rebuild of a particular release is planned; this is marked with the label "Not scheduled." A device running any release in the given train that is earlier than the release in a specific column (less than the earliest fixed release) is known to be vulnerable, and it should be upgraded at least to the indicated release or a later version (greater than the earliest fixed release label).

When selecting a release, keep in mind the following definitions:

- **Maintenance**

Most heavily tested and highly recommended release of any label in a given row of the table.

- **Rebuild**

Constructed from the previous maintenance or major release in the same train, it contains the fix for a specific vulnerability. Although it receives less testing, it contains only the minimal changes necessary to effect the repair. Cisco has made available several rebuilds of mainline trains to address this vulnerability, but strongly recommends running only the latest maintenance release on mainline trains.

- **Interim**

Built at regular intervals between maintenance releases and receives less testing. Interims should be selected only if there is no other suitable release that addresses the vulnerability, and interim images should be upgraded to the next available maintenance release as soon as possible. Interim releases are not available through manufacturing, and usually they are not available for customer download from CCO without prior arrangement with the Cisco Technical Assistance Center (TAC).

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 TAC for assistance, as shown in the section following this table.

Train	Description of Image or Platform	Availability of Fixed Releases		
10.x-based Releases		Not scheduled		
11.x-based Releases		Rebuild	Interim	Maintenance
11.0		Not scheduled – Migrate to 11.1 or later		
11.1		11.1(24c)**		
11.1AA		11.1(20)AA5		
11.1CA		11.1(36)CA4**		
11.1CC		11.1(36)CC7		
11.2		11.2(15b)**		
		11.2(26e)**		
11.2P		11.2(17)P1**		
		11.2(20)P1**		
		11.2(26)P5**		
11.2SA	Catalyst 2900XL 4MB	11.2(8.11)SA6		
11.3		11.3(11d)		

11.3T		11.3(11b)T3		
12.0-based Releases		Rebuild	Interim	Maintenance
12.0	General Deployment release for all platforms	12.0(19b)**, 12.0(16b)**, 12.0(15b), 12.0(8b)**		12.0(26)
12.0DA	xDSL support: 6100, 6200	Migrate to 12.2DA; 12.2(10)DA2, 12.2(12)DA3, Engineering Specials available on request.		
12.0DB	Early Deployment 6400 UAC for NSP	Migrate to 12.3(1a)		
12.0DC	Early Deployment 6400 UAC for NRP	Migrate to 12.3(1a)		
12.0S	Core/ISP support: GSR, RSP, c7200, c10k	12.0(24)S2 12.0(23)S3 12.0(22)S5 12.0(21)S7 12.0(19)S4 12.0(18)S7 12.0(17)S7 12.0(16)S10 12.0(15)S7 12.0(14)S8 12.0(13)S8 12.0(12)S4 12.0(10)S8 12.0(21)S4a** 12.0(10)S3b** 12.0(16)S8a** 12.0(19)S2a** 12.0(21)S5a** 12.0(18)S5a**		12.0(25)S – Image is under a Software Advisory, but is NOT VULNERABLE.
12.0SC	Cable/broadband ISP: uBR7200	Migrate to 12.1(19)EC		Recommended version is 12.0(25)S1

12.0SL	10000ESR: c10k	Migrate to 12.0(23)S3, 12.0(17)SL9**		
12.0SP	Early Deployment	Migrate to 12.0(22)S5, 12.0(21)SP4** is available		
12.0ST	Early Deployment release for Core/ISP support: GSR, RSP, c7200	12.0(21)ST7, 12.0(20)ST6, 12.0(19)ST6, 12.0(17)ST8, 12.0(21)ST3a**		
12.0SX	12.0(21)SX	Migrate to 12.0(22)S5		
	12.0(22)SX			
12.0SY	Early Deployment	Migrate to 12.0(23)S3		
12.0SZ	Early Deployment	Migrate to 12.0(23)S3		
12.0T	Early Deployment	12.0(7)T3		
12.0W5	Cat8510c, cat8510m, cat8540c, cat8540m, ls1010	12.0(24)W5(26c)**		12.0(26)W5(28)
	Cat2950	Migrate to 12.1(13)EA1c		
	Cat4232 and Cat2948G-L3	12.0(25)W5(27)		
	C6MSM	Engineering Special available on request		
	C5rsfc, C5rsm, C3620, C3640, C4500, C7200, RSP			12.1(20)
12.0WC	Early deployment 2900XL-LRE, 2900XL/3500XL	12.0(5)WC8		
12.0WT	Early deployment Catalyst switches: cat4840g	Engineering Special Available upon request		
12.0X(l)	Short-lived Early Deployment Releases	All 12.0X(any letter) releases have migrated to either 12.0T or 12.1 unless otherwise documented in the X release technical notes pertaining to the specific release. Please check migration paths for all 12.0X releases.		
12.1-based Releases		Rebuild	Interim	Maintenance
12.1	General Deployment release for all platforms	12.1(17a)**		
		12.1(4b)**		
		12.1(6b)**		
		12.1(13a)	12.1(18.4)	12.1(19)
12.1AA		Migrate to 12.2		
12.1AX	Catalyst 3750, Catalyst 2970	12.1(14)EA1 – Jul-28-2003 Engineering special available upon request		

12.1AY	Catalyst 2940			12.1(13)AY
12.1DA	6160 platform	Migrate to 12.2DA		
12.1DB	6400 UAC	12.1(5)DB2		Migrate to 12.3(1a)
12.1DC	6400 UAC	12.1(5)DC3		Migrate to 12.3(1a)
12.1E	Core Enterprise support – c7200, Catalyst 6000, RSP, c7100, Cat4000, Cat8500MSR, Cat8500CSR, LS1010, and ONS15540	12.1(6)E12** 12.1(7a)E1a** 12.1(8b)E14 12.1(11b)E12 12.1(12c)E7** 12.1(13)E7 –Image has been deferred but is NOT VULNERABLE. Recommended release is 12.1(13)E8 12.1(14)E4 12.1(10)E6a** 12.1(11b)E0a** 12.1(7)E0a**		12.1(19)E
12.1EA	12.1(4)EA 12.1(6)EA 12.1(8)EA 12.1(9)EA 12.1(11)EA 12.1(12c)EA 12.1(13)EA	Migrate to 12.1(13)EA1c		
12.1EB	LS1010			12.1(14)EB
12.1EC	Early Deployment	12.1(13)EC4		12.1(19)EC (August–25–2003)
12.1EV	Early Deployment	12.1(12c)EV2		
12.1EW	Early Deployment Cat4000 L3	12.1(12c)EW2 12.1(13)EW2		12.1(19)EW

12.1EX	Early Deployment	12.1(1)EX to 12.1(8b)EX5 Migrate to 12.1(8b)E14 12.1(9)EX to current – To be determined		
12.1EY				Migrate to 12.1(14)E4 Migrate to 12.1(14)EB (LS1010 ONLY)
12.1YJ		12.1(14)EA1 – Jul–28–2003		
12.1T	Early Deployment	12.1(5)T8c** 12.1(5)T15		
12.1X(l)	12.1X releases generally migrate to 12.1T, 12.2 or 12.2T as specified below. Please refer to specific train Technical notes for documented migration path.			
12.1XA	Short-lived Early Deployment Release	Migrate to 12.2(11)T9		
12.1XC 12.1XD 12.1XH	Short-lived Early Deployment Releases	Migrate to 12.2(17)		
12.1XI		12.1(3a)XI9**		
12.1XB 12.1XF 12.1XG 12.1XJ 12.1XL 12.1XP 12.1XR 12.1XT 12.1YB 12.1YC 12.1YD 12.1YH	Short-lived Early Deployment Releases	Migrate to 12.2(15)T5		
12.1XM 12.1XQ 12.1XV	Short-lived Early Deployment Releases	Migrate to 12.2(2)XB11		
12.1XU	Short-lived Early Deployment Release	Migrate to 12.2(4)T6		
12.1YE 12.1YF 12.1YI	Short-lived Early Deployment Releases	Migrate to 12.2(2)YC		
12.2-based Releases		Rebuild	Interim	Maintenance
12.2	General Deployment (GD) candidate for all platforms	12.2(16a), 12.2(13b)M2**, 12.2(12e), 12.2(10d),		12.2(17)

		12.2(6j), 12.2(7g)**		
12.2B	12.2(2)B–12.2(4)B7	12.2(4)B7a**		Migrate to 12.3(1a)
	12.2(4)B8–12.2(16)B	12.2(16)B1		
12.2BC	Early Deployment Release	12.2(15)BC1 – (Scheduled for August 2003) 12.2(11)BC3c		
12.2BW	Early Deployment for use with 7200, 7400, and 7411 platforms	Migrate to 12.3(1a)		
12.2BX	Broadband/Leased line			12.2(16)BX
12.2BZ	Early Deployment Release	12.2(15)BZ1** (Available in August–2003)		Migrate to 12.2(16)BX
12.2CX	Early Deployment Release	Migrate to 12.2(15)BC1		
12.2CY	Early Deployment Release	Migrate to 12.2(15)BC1		
12.2DA	Early Deployment Release	12.2(10)DA2, 12.2(12)DA3, Engineering Special available on request		
12.2DD	Early Deployment Release	Migrate to 12.3(1a)		
12.2DX	Early Deployment Release	Migrate to 12.3(1a)		
12.2JA	Cisco Aironet hardware platforms: Introduction of Access Point feature in IOS, Cisco 1100 Series Access Point (802.11b)			12.2(11)JA
12.2MB	Specific Technology ED for 2600 7500 (GPRS/PDSN/GGSN 2600/7200/7500)	12.2(4)MB12		
12.2MC	Early Deployment: IP RAN	12.2(15)MC1 available September–2003		
12.2MX		12.2(8)YD		
12.2S	Core/ISP support: RSP, c7200	12.2(14)S1	12.2(16.5)S	
12.2SX	IOS Support for C6500 Supervisor720	12.2(14)SX1		
12.2SY	VPN feature release for c6k/76xx VPN service module	12.2(14)SY1 – Aug–4–2003 12.2(8)YD		
12.2SZ	7304 Platform	12.2(14)SZ2		
12.2T	New Technology Early Deployment (ED) release for all platforms	12.2(15)T5,12.2(13)T5, 12.2(11)T9,12.2(8)T10, 12.2(4)T6,	12.2(16.5)T	No more maintenance trains for 12.2T are

		12.2(8)T0c**, 12.2(13)T1a**		planned. Please migrate to the latest 12.3 Mainline release.
12.2X(l) 12.2Y(l)	Short-lived Early Deployment Releases	Many short-lived releases migrate to the same train; the trains below this point until the following section are not grouped by strict alphabetical order, but are grouped by migration path. Please review documented migration paths for your trains.		
12.2XA	Short-lived Early Deployment Releases	Migrate to 12.2(11)T9		
12.2XM		Migrate to 12.2(4)YA6		
12.2XS		12.2(2)XB11		Migrate to 12.2(2)XB11
		12.2(1)XS1a**		
12.2XD 12.2XE 12.2XH 12.2XI 12.2XJ 12.2XK 12.2XL 12.2XQ 12.2XU 12.2XW 12.2YB 12.2YC 12.2YF 12.2YG 12.2YH 12.2YJ 12.2YT	Short-lived Early Deployment Releases	Migrate to 12.2(15)T5		
12.2YA		12.2(4)YA6		
12.2YN	Short-lived Early Deployment Release	Migrate to 12.2(13)ZH2 – July–25–2003		
12.2YO	Short-lived Early Deployment Release	Migrate to 12.2(14)SY1 available Aug–4–2003: Engineering Special available on request		
12.2XB	Early Deployment Release with continuing support	12.2(2)XB11		
12.2XC	Short-lived Early Deployment Release	Migrate to 12.2(8)ZB7 – Jul–24–2003		
12.2XF	Short-lived Early Deployment Release uBR10000	Migrate to 12.2(15)BC1		
12.2XG	Short-lived Early Deployment Release	Migrate to 12.2(8)T10		
		Migrate to 12.2(11)T9		

12.2XN 12.2XT	Short-lived Early Deployment Releases			
12.2YD	Short-lived Early Deployment Release	Migrate to 12.2(8)YY		
12.2YK		Migrate to 12.2(13)ZC		
12.2YL 12.2YM 12.2YU 12.2YV	Short-lived Early Deployment Releases	Migrate to 12.2(13)ZH2 – July-25-2003		
12.2YP	Short-lived Early Deployment Release	12.2(11)YP1**		
12.2YQ 12.2YR	Short-lived Early Deployment Releases	Migrate to 12.2(15)ZL		
12.2YS	Short-lived Early Deployment Release	12.2(15)YS/1.2(1)		
12.2YW	Short-lived Early Deployment Release	12.2(8)YW2		
12.2YX	Short-lived Early Deployment Release Crypto for 7100/7200	12.2(11)YX1		
12.2YY	Short lived Early Deployment Releases IOS support for General Packet Radio Service	12.2(8)YY3		
12.2YZ	Short-lived Early Deployment Release	12.2(11)YZ2		
12.2ZA	Short-lived Early Deployment Release			12.2(14)ZA2
12.2ZB	Short-lived Early Deployment Release	12.2(8)ZB7		
12.2ZC	Short-lived Early Deployment Release			12.2(13)ZC
12.2ZD	Short-lived Early Deployment Release	Not Scheduled		
12.2ZE	Short-lived Early Deployment Release	12.3(1a)		
12.2ZF	Short-lived Early Deployment Release	12.2(13)ZF1		
12.2ZG	Short-lived Early Deployment Release	Migrate to 12.2(13)ZH2 – July-25-2003		
12.2ZH	Short-lived Early Deployment Release	12.2(13)ZH2		
12.2ZJ	Short-lived Early Deployment Release	12.2(15)ZJ1		

12.2ZL	Short-lived Early Deployment Release	Not Vulnerable		
12.3-based Releases		NOT VULNERABLE		

Notes:

** Marked versions of code are not available on CCO. Please contact the Cisco TAC and request the specific images you need posted.

Cisco ONS 15454 Software

This vulnerability is repaired in Cisco ONS 15454 Software Release 4.1.0 and later and is expected to be available in early August, 2003.

Obtaining Fixed Software

Customers with contracts should obtain upgraded software free of charge through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on the Cisco worldwide website at <http://www.cisco.com/tacpage/sw-center/sw-ios.shtml>.

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 obtaining the free software upgrade(s).

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. To ensure prompt service by email or by phone, please provide your name, company name, address, product serial number, and current version of Cisco IOS software that you are using. This can be documented by pasting the output of the **show version** command into the text of an email. 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, instructions, and e-mail addresses for use in various languages.

Workarounds

Cisco recommends that all IOS devices which process IPv4 packets be configured to block unwanted traffic, or any traffic directed to the router from an unauthorized source with the use of Access Control Lists (ACLs). This can be done at multiple locations, and it is recommended that you review all methods and use the

combination which fits your network best. Although the following ACLs are listed as a workaround for this vulnerability, in cases where performance is not impacted, these techniques can be considered best practices and may be left in place as a long-term solution rather than a temporary fix.

Best practices dictate that legitimate traffic is defined as management protocols such as telnet, snmp, or ssh, and configured routing protocols from explicitly allowed peers. All other traffic destined to the device should be blocked at the input interface. Traffic entering the network should also be carefully evaluated and filtered at the network edge if destined to an infrastructure device. Although network service providers must often allow unknown traffic to transit their network, it is not necessary to allow that same traffic destined to their network infrastructure. Several white papers have been written to assist in deploying these recommended security best practices.

For devices with interfaces that are currently blocked due to exploitation of this vulnerability, ACL workarounds may be applied. AFTER APPLYING THE WORKAROUND, the input queue depth may be raised with the **hold-queue <new value> in** interface command to something larger than the default size of 75. This will allow traffic flow on the interface. The device may then be reloaded at a convenient time to release the blocked packets.

For interfaces blocked with PIM packets only, the PIM process may be enabled on the router after applying a workaround which will clear protocol type 103 packets from the blocked input queue. This does not clear packets with protocol type 53, 55, or 77 from the input queue. Although a device with PIM enabled is not vulnerable to attacks with protocol 103 packets, enabling PIM is not recommended as a workaround to this vulnerability, as it does not block protocols 53, 55, or 77, and may have performance implications.

ACLs can have performance impact on certain platforms, so care should be taken when applying the recommended workarounds.

Transit ACLs

The following access list is specifically designed to block attack traffic. Note that the attack traffic can include spoofed source addresses. This access list should be applied to **all** interfaces of the device, both entering and leaving your network, and should include topology-specific filters. This could include filtering routing protocol traffic, management protocols, and traffic destined for the internal network. Protocol 103 is Protocol Independent Multicast (PIM), which is a commonly deployed application in multicast networks. Interfaces with PIM enabled have not been found to be vulnerable to exploit traffic with protocol 103; PIM traffic may be permitted to those select devices.

```
access-list 101 permit tcp any any
access-list 101 permit udp any any
access-list 101 deny 53 any any
access-list 101 deny 55 any any
access-list 101 deny 77 any any
access-list 101 deny 103 any any
!--- insert any other previously applied ACL entries here
!--- you must permit other protocols through to allow normal
!--- traffic -- previously defined permit lists will work
!--- or you may use the permit ip any any shown here
access-list 101 permit ip any any
```

Prior to deploying ACLs that filter transit traffic, a classification ACL can be used to help identify required permit statements. A classification ACL is an ACL that permits a series of protocols. Displaying access-list entry hit counters helps determine required protocols: entries with zero packets counted are likely not required. Classification access-lists are detailed in the link below for infrastructure access-lists.

Receive ACLs

For distributed platforms, receive path access lists may be an option starting in Cisco IOS Software Versions 12.0(21)S2 for the c12000 and 12.0(24)S for the c7500. The receive access lists protect the device from harmful traffic before the traffic can impact the route processor. Receive path 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 CPU load is distributed to the line card processors and helps mitigate load on the main route processor. The white paper entitled "GSR: Receive Access Control Lists" will help you identify and allow legitimate traffic to your device and deny all unwanted packets:

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

Infrastructure ACLs

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 entitled "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>

Exploitation and Public Announcements

Since the initial posting of this document, the Cisco PSIRT has been made aware of public announcements of the vulnerabilities described in this advisory. Cisco PSIRT is aware that the exploit for this vulnerability has been published on a public mailing list.

Status of This Notice: INTERIM

This is an INTERIM notice. Although Cisco cannot guarantee the accuracy of all statements in this notice, all of the facts have been checked to the best of our ability. Cisco does not anticipate issuing updated versions of this advisory unless there is some material change in the facts. Should there be a significant change in the facts, Cisco will update this advisory.

Distribution

This notice is posted on the Cisco worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.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 at the public release date and time:

- cust-security-announce@cisco.com
- bugtraq@securityfocus.com
- full-disclosure@lists.netsys.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- nanog@merit.edu
- sanog@sanog.org

- comp.dcom.sys.cisco
- Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on the Cisco worldwide web server. Users concerned about this problem are encouraged to check the URL given above for any updates.

Revision History

Revision 1.0	17-July-2003 0:00 GMT	Initial public release
Revision 1.1	17-July-2003 6:10 GMT	Updated Workaround section (access lists), Updated table with information on 12.0W5
Revision 1.2	17-July-2003 10:30 GMT	Corrected "Last Updated" time; corrected document title of Infrastructure ACL link under Workaround section
Revision 1.3	17-July-2003 23:00 GMT	Added "with specific protocol fields" in Summary section; updated Details section to include protocol types; added details to the Cisco vulnerabilities paragraph; added an output example to identify an attack packet; rewrote Transit ACLs section; updated Exploitation and Public Announcements paragraph
Revision 1.4	18-July-2003 10:00 GMT	Added sentence in Exploitation and Public Announcements section
Revision 1.5	18-July-2003 14:00 GMT	Added information about the PIM process and modified output in the Details section
Revision 1.6	18-July-2003 21:00 GMT	Fixed links to iacl and tacl document; Changed 11.2SA, 12.0S, 12.0SX, 12.0WC, 12.1AX, 12.1E, 12.1XA, 12.2BC, 12.2DA, 12.2SX, 12.2SY, 12.2XC, 12.ZB
Revision 1.7	21-July-2003 05:00 GMT	Reformatted Workaround section; added recommendations about security best practices; included PIM-specific workaround; clarified details about bugs; confirmed that non-Ethernet interfaces are affected; confirmed Cisco switches/line cards that run IOS are affected.

Revision 1.8	22–July–2003 14:38 GMT	Added available software fixes for 11.1, 11.1CC, 12.0, 12.0S, 12.0SP, 12.1, 12.2ZF, 12.2ZG, and 12.2ZH.
Revision 1.9	22–July–2003 23:15 GMT	Added affected product of ONS 15454 ML–series cards, added link to network management whitepaper, and updated available software fixes for 11.1, 12.0S, 12.0ST, 12.0W5, 12.1, 12.1E, 12.1EV, 12.1EW, 12.1EX, 12.1EY, 12.1T, 12.2, 12.2BC, 12.2CX, 12.2CY, and 12.2T.
Revision 1.10	24–July–2003 22:34 UTC (GMT)	Updated workarounds, and updated available software fixes for 11.1, 11.3, 11.3T, 12.0S, 12.0SL, 12.0W5, 12.1E, 12.1EC, 12.1T, 12.1XI, 12.2BZ, 12.2DA, 12.2XM, 12.2YA, 12.2YN, 12.2ZF, 12.2ZG, 12.2ZH, 12.2YL, 12.2YM, 12.2YU, and 12.2YV.
Revision 1.11	30–July–2003 14:45 UTC (GMT)	Updated available software fixes for 11.1AA, 11.2, 11.2P, 12.0, 12.1, 12.1E, 12.1EC, 12.1T, 12.2, 12.2B, 12.2BZ, 12.2MC, 12.2T, 12.2XS, 12.2YA, 12.2YP, 12.2ZB, 12.2ZF, 12.2ZH
Revision 1.12	31–July–2003 15:45 UTC (GMT)	Updated available software fixes for 11.2
Revision 1.13	02–August–2003 01:00 UTC (GMT)	Updated available software fixes for 12.0T and 12.1EC
Revision 1.14	04–September–2003 18:16 UTC (GMT)	Updated available software fixes for 12.0 and 12.2
Revision 1.15	22–July–2004 20:00 UTC (GMT)	Fixed broken URL under Affected Products 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 the Cisco worldwide website at http://www.cisco.com/warp/public/707/sec_incident_response.shtml. This includes instructions for press inquiries regarding Cisco security notices.

All Cisco Security Advisories are available at <http://www.cisco.com/go/psirt>.