

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-01/msg00020.html>

- *From:* Cisco Systems Product Security Incident Response Team <psirt@xxxxxxxx>
 - *Date:* Wed, 24 Jan 2007 16:12:00 -0000
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

Advisory ID: cisco-sa-20070124-crafted-tcp

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml>

Revision 1.0

For Public Release 2007 January 24 1600 UTC (GMT)

Summary

=====

The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

Cisco has made free software available to address this vulnerability for affected customers.

This issue is documented as Cisco bug ID CSCek37177.

There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml>

Affected Products

=====

Vulnerable Products

+-----

This issue affects all Cisco devices running Cisco IOS software. To be affected, devices must be configured to process Internet Protocol version 4 (IPv4) packets and receive TCP packets. Devices which run only Internet Protocol version 6 (IPv6) are not affected.

This vulnerability is present in all unfixed versions of Cisco IOS software, including versions 9.x, 10.x, 11.x and 12.x.

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 Cisco IOS release 12.2(14)S16 with an installed image name of C7200-IS-M:

```
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-IS-M), Version 12.2(14)S16, RELEASE SOFTWARE (fc1)
```

The release train label is "12.2".

The next example shows a product running IOS release 12.3(7)T12 with an image name of C7200-IK9S-M:

```
Cisco IOS Software, 7200 Software (C7200-IK9S-M), Version 12.3(7)T12, RELEASE SOFTWARE (fc1)
```

Additional information about Cisco IOS Banners is available at:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml#3

Products Confirmed Not Vulnerable

+-----

Cisco products that do not run IOS are unaffected by this vulnerability.

Cisco IOS-XR is not affected.

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

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

Details

=====

TCP is the transport layer protocol designed to provide connection-oriented, reliable delivery of a data stream. To accomplish this, TCP uses a mixture of flags to indicate state and sequence numbers to identify the order in which the packets are to be reassembled. TCP also provides a number, called an acknowledgement number, that is used to indicate the sequence number of the next packet expected. The full specification of the TCP protocol can be found at <http://www.ietf.org/rfc/rfc0793.txt>

Cisco IOS devices that are configured to receive TCP packets are exposed to this issue. This Advisory does not apply to traffic that is transiting the device.

Certain crafted packets destined to an IPv4 address assigned to a physical or virtual interface on a Cisco IOS device may cause the device to leak a small amount of memory. Over time, such a memory leak may lead to memory exhaustion and potentially degraded service.

Although this is an issue with TCP, it is not required to complete the TCP 3-way handshake in order for the memory leak to be triggered. Therefore, TCP packets with a spoofed source address may trigger the leak.

The following document contains additional information on how to identify if your router is suffering from a memory leak in Processor memory:

<http://www.cisco.com/warp/public/63/mallocfail.shtml#tshoot2>

Vulnerability Scoring Details

=====

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). Cisco will provide a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias parameter when determining the environmental impact of a particular vulnerability.

CVSS is a standards based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

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:

<http://intellishield.cisco.com/security/alertmanager/cvss>

Cisco Bug IDs:

CSCek37177

CVSS Base Score: 3.3

Access Vector: Remote

Access Complexity: Low

Authentication: Not Required

Confidentiality Impact: None

Integrity Impact: None

Availability Impact: Complete

Impact Bias: Normal

CVSS Temporal Score: 2.7

Exploitability: Functional

Remediation Level: Official Fix

Report Confidence: Confirmed

Impact

=====

Successful exploitation of the vulnerability may result in a small amount of processor memory to leak, which may lead to degraded service. This issue will not resolve over time, and will require a device reset to recover the leaked memory.

This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the device will not trigger this issue.

Software Version 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.

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

Each row of the Cisco IOS software table (below) describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

For more information on the terms "Rebuild" and "Maintenance," consult the following URL:

<http://www.cisco.com/warp/public/620/1.html>

Major Release	Availability of Repaired Releases	Affected	12.0-Based Release	Rebuild	Maintenance
12.0	Vulnerable; migrate to 12.2(37) or later				
12.0DA	Vulnerable; migrate to 12.2(10)DA5 or later				
12.0DB	Vulnerable; migrate to 12.3(4)T13 or later				
12.0DC	Vulnerable; migrate to 12.3(4)T13 or later				
12.0(31)S6					
12.0S					
12.0(32)S4					
12.0SC	Vulnerable; migrate to 12.3(13a)BC6 or later				
12.0SL	Vulnerable; migrate to 12.0(31)S6 or later				
12.0SP	Vulnerable; migrate to 12.0(31)S6 or later				
12.0ST	Vulnerable; migrate to 12.0(31)S6 or later				
12.0SX	12.0(25)SX11				
12.0SY	12.0(32)SY				
12.0SZ	Vulnerable; migrate to 12.0(31)S6 or later				

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

12.0T Vulnerable; migrate to 12.2(37) or later
-----+-----
12.0W Not vulnerable
-----+-----
12.0WC 12.0(5)WC15
-----+-----
12.0WT Not vulnerable
-----+-----
12.0XA Vulnerable; migrate to 12.2(37) or later
-----+-----
12.0XB Vulnerable; migrate to 12.2(37) or later
-----+-----
12.0XC Vulnerable; migrate to 12.2(37) or later
-----+-----
12.0XD Vulnerable; migrate to 12.2(37) or later
-----+-----
12.0XE Vulnerable; migrate to 12.1(26)E7 or later
-----+-----
12.0XF Not vulnerable
-----+-----
12.0XG Vulnerable; migrate to 12.2(37) or later
-----+-----
12.0XH Vulnerable; migrate to 12.2(37) or later
-----+-----
12.0XI Vulnerable; migrate to 12.2(37) or later
-----+-----
12.0XJ Vulnerable; migrate to 12.2(37) or later
-----+-----
12.0XK Vulnerable; migrate to 12.2(37) or later
-----+-----
12.0XL Vulnerable; migrate to 12.2(37) or later
-----+-----
12.0XM Vulnerable; migrate to 12.2(37) or later
-----+-----
12.0XN Vulnerable; migrate to 12.2(37) or later
-----+-----
12.0XQ Vulnerable; migrate to 12.2(37) or later
-----+-----
12.0XR Vulnerable; migrate to 12.2(37) or later
-----+-----
12.0XS Vulnerable; migrate to 12.1(26)E7 or later
-----+-----
12.0XV Vulnerable; migrate to 12.2(37) or later
-----+-----
12.0XW Not vulnerable
-----+-----
Affected
12.1–Based Rebuild Maintenance
Release
-----+-----
12.1 Vulnerable; migrate to 12.2(37) or later

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

12.1 AA	Vulnerable; migrate to 12.2(37) or later
12.1 AX	Vulnerable; migrate to 12.2(25)EY4 or later
12.1 AY	Vulnerable; migrate to 12.1(22)EA8 or later
12.1 AZ	Vulnerable; migrate to 12.1(22)EA8 or later
12.1 CX	Vulnerable; migrate to 12.2(37) or later
12.1 DA	Vulnerable; migrate to 12.2(10)DA5 or later
12.1 DB	Vulnerable; migrate to 12.3(4)T13 or later
12.1 DC	Vulnerable; migrate to 12.3(4)T13 or later
12.1(26)E7	
12.1E	
12.1(27b)E1	
12.1EA	12.1(22)EA8
12.1EB	Vulnerable; contact TAC
12.1EC	Vulnerable; migrate to 12.3(13a)BC6 or later
12.1(19)EO6	available on
12.1EO	31-Jan-07
12.1(20)EO3	
12.1EU	Vulnerable; migrate to 12.2(25)EWA6 or later
12.1EV	Vulnerable; migrate to 12.2(27)SV4 or later
12.1EW	Vulnerable; migrate to 12.2(25)EWA6 or later
12.1EX	Vulnerable; migrate to 12.1(26)E7 or later
12.1EY	Vulnerable; migrate to 12.1(26)E7 or later
12.1EZ	Vulnerable; migrate to 12.1(26)E7 or later
12.1T	Vulnerable; migrate to 12.2(37) or later
12.1XA	Vulnerable; migrate to 12.2(37) or later
12.1XB	Vulnerable; migrate to 12.2(37) or later
12.1XC	Vulnerable; migrate to 12.2(37) or later

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

12.1XD	Vulnerable; migrate to 12.2(37) or later
12.1XE	Vulnerable; migrate to 12.1(26)E7 or later
12.1XF	Vulnerable; migrate to 12.3(19) or later
12.1XG	Vulnerable; migrate to 12.3(19) or later
12.1XH	Vulnerable; migrate to 12.2(37) or later
12.1XI	Vulnerable; migrate to 12.2(37) or later
12.1XJ	Vulnerable; migrate to 12.3(19) or later
12.1XL	Vulnerable; migrate to 12.3(19) or later
12.1XM	Vulnerable; migrate to 12.3(19) or later
12.1XP	Vulnerable; migrate to 12.3(19) or later
12.1XQ	Vulnerable; migrate to 12.3(19) or later
12.1XR	Vulnerable; migrate to 12.3(19) or later
12.1XS	Vulnerable; migrate to 12.2(37) or later
12.1XT	Vulnerable; migrate to 12.3(19) or later
12.1XU	Vulnerable; migrate to 12.3(19) or later
12.1XV	Vulnerable; migrate to 12.3(19) or later
12.1XW	Vulnerable; migrate to 12.2(37) or later
12.1XX	Vulnerable; migrate to 12.2(37) or later
12.1XY	Vulnerable; migrate to 12.2(37) or later
12.1XZ	Vulnerable; migrate to 12.2(37) or later
12.1YA	Vulnerable; migrate to 12.3(19) or later
12.1YB	Vulnerable; migrate to 12.3(19) or later
12.1YC	Vulnerable; migrate to 12.3(19) or later
12.1YD	Vulnerable; migrate to 12.3(19) or later
12.1YE	Vulnerable; migrate to 12.3(19) or later

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

12.1YF	Vulnerable; migrate to 12.3(19) or later
12.1YH	Vulnerable; migrate to 12.3(19) or later
12.1YI	Vulnerable; migrate to 12.3(19) or later
12.1YJ	Vulnerable; migrate to 12.1(22)EA8 or later
Affected	
12.2-Based	Rebuild Maintenance Release
12.2	12.2(37)
12.2B	Vulnerable; migrate to 12.3(4)T13 or later
12.2BC	Vulnerable; migrate to 12.3(13a)BC6 or later
12.2BW	Vulnerable; migrate to 12.3(19) or later
12.2BY	Vulnerable; migrate to 12.3(4)T13 or later
12.2BZ	Vulnerable; migrate to 12.3(7)XI8 or later
12.2CX	Vulnerable; migrate to 12.3(13a)BC6 or later
12.2CY	Vulnerable; migrate to 12.3(13a)BC6 or later
12.2CZ	Vulnerable; contact TAC
12.2(10)DA5	
12.2DA	
12.2(12)DA10	
12.2DD	Vulnerable; migrate to 12.3(4)T13 or later
12.2DX	Vulnerable; migrate to 12.3(4)T13 or later
12.2EU	Vulnerable; migrate to 12.2(25)EWA6 or later
12.2EW	Vulnerable; migrate to 12.2(25)EWA6 or later
12.2EWA	12.2(25)EWA6
12.2EX	12.2(25)EX1
12.2EY	12.2(25)EY4
12.2EZ	Vulnerable; migrate to 12.2(25)SEE1 or later
12.2FX	Vulnerable; migrate to 12.2(25)SEE1 or later

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

12.2FY	Vulnerable; migrate to 12.2(25)SEE1 or later
12.2FZ	All 12.2FZ releases are fixed
12.2IXA	Vulnerable; contact TAC
12.2IXB	Vulnerable; contact TAC
12.2IXC	Vulnerable; contact TAC
12.2JA	Vulnerable; migrate to 12.3(8)JA2 or later
12.2JK	Vulnerable; migrate to 12.4(4)T4 or later
12.2MB	Vulnerable; migrate to 12.2(25)SW8 or later
12.2MC	Vulnerable; migrate to 12.3(11)T11 or later
12.2S	12.2(25)S12; Available 12-Feb-07
12.2SB	12.2(28)SB2 12.2(31)SB
12.2SBC	12.2(27)SBC5
12.2SE	12.2(35)SE
12.2SEA	Vulnerable; migrate to 12.2(25)SEE1 or later
12.2SEB	Vulnerable; migrate to 12.2(25)SEE1 or later
12.2SEC	Vulnerable; migrate to 12.2(25)SEE1 or later
12.2SED	Vulnerable; migrate to 12.2(25)SEE1 or later
12.2SEE	12.2(25)SEE1
12.2SEF	12.2(25)SEF1
12.2SEG	All 12.2SEG releases are fixed
12.2SG	Vulnerable; contact TAC
12.2SGA	All 12.2SGA releases are fixed
12.2SO	12.2(18)SO7
12.2SRA	All 12.2SRA releases are fixed
12.2SRB	All 12.2SRB releases are fixed

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

12.2SU	Vulnerable; migrate to 12.4(8) or later
12.2(27)SV4	
12.2SV	12.2(28)SV1
12.2(29)SV1	
12.2SW	12.2(25)SW8
12.2SX	Vulnerable; migrate to 12.2(18)SXD7a or later
12.2SXA	Vulnerable; migrate to 12.2(18)SXD7a or later
12.2SXB	Vulnerable; migrate to 12.2(18)SXD7a or later
12.2SXD	12.2(18)SXD7a
12.2SXE	12.2(18)SXE6
12.2SXF	12.2(18)SXF5
12.2SY	Vulnerable; migrate to 12.2(18)SXD7a or later
12.2SZ	Vulnerable; migrate to 12.2(25)S12 or later; Available 12-Feb-07
12.2T	Vulnerable; migrate to 12.3(19) or later
12.2TPC	Vulnerable; contact TAC
12.2XA	Vulnerable; migrate to 12.3(19) or later
12.2XB	Vulnerable; migrate to 12.3(19) or later
12.2XC	Vulnerable; migrate to 12.3(4)T13 or later
12.2XD	Vulnerable; migrate to 12.3(19) or later
12.2XE	Vulnerable; migrate to 12.3(19) or later
12.2XF	Vulnerable; migrate to 12.3(13a)BC6 or later
12.2XG	Vulnerable; migrate to 12.3(19) or later
12.2XH	Vulnerable; migrate to 12.3(19) or later
12.2XI	Vulnerable; migrate to 12.3(19) or later
12.2XJ	Vulnerable; migrate to 12.3(19) or later

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

12.2XK	Vulnerable; migrate to 12.3(19) or later
12.2XL	Vulnerable; migrate to 12.3(19) or later
12.2XM	Vulnerable; migrate to 12.3(19) or later
12.2XN	Vulnerable; migrate to 12.3(19) or later
12.2XQ	Vulnerable; migrate to 12.3(19) or later
12.2XR	Vulnerable; migrate to 12.3(19) or later
12.2XS	Vulnerable; migrate to 12.3(19) or later
12.2XT	Vulnerable; migrate to 12.3(19) or later
12.2XU	Vulnerable; migrate to 12.3(19) or later
12.2XV	Vulnerable; migrate to 12.3(19) or later
12.2XW	Vulnerable; migrate to 12.3(19) or later
12.2YA	Vulnerable; migrate to 12.3(19) or later
12.2YB	Vulnerable; migrate to 12.3(19) or later
12.2YC	Vulnerable; migrate to 12.3(19) or later
12.2YD	Vulnerable; migrate to 12.3(11)T11 or later
12.2YE	Vulnerable; migrate to 12.2(25)S12 or later; Available 12-Feb-07
12.2YF	Vulnerable; migrate to 12.3(19) or later
12.2YG	Vulnerable; migrate to 12.3(19) or later
12.2YH	Vulnerable; migrate to 12.3(19) or later
12.2YJ	Vulnerable; migrate to 12.3(19) or later
12.2YK	Vulnerable; migrate to 12.3(4)T13 or later
12.2YL	Vulnerable; migrate to 12.3(4)T13 or later
12.2YM	Vulnerable; migrate to 12.3(4)T13 or later
12.2YN	Vulnerable; migrate to 12.3(4)T13 or later
12.2YO	Not vulnerable

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

12.2YP	Vulnerable; migrate to 12.3(19) or later
12.2YQ	Vulnerable; migrate to 12.3(4)T13 or later
12.2YR	Vulnerable; migrate to 12.3(4)T13 or later
12.2YS	Not vulnerable
12.2YT	Vulnerable; migrate to 12.3(19) or later
12.2YU	Vulnerable; migrate to 12.3(4)T13 or later
12.2YV	Vulnerable; migrate to 12.3(4)T13 or later
12.2YW	Vulnerable; migrate to 12.3(4)T13 or later
12.2YX	Vulnerable; migrate to 12.4(8) or later
12.2YY	Vulnerable; migrate to 12.3(4)T13 or later
12.2YZ	Vulnerable; migrate to 12.2(25)S12 or later; Available 12-Feb-07
12.2ZA	Vulnerable; migrate to 12.2(18)SXD7a or later
12.2ZB	Vulnerable; migrate to 12.3(4)T13 or later
12.2ZC	Vulnerable; migrate to 12.3(4)T13 or later
12.2ZD	Vulnerable; contact TAC
12.2ZE	Vulnerable; migrate to 12.3(19) or later
12.2ZF	Vulnerable; migrate to 12.3(4)T13 or later
12.2ZG	Vulnerable; contact TAC
12.2ZH	Vulnerable; contact TAC
12.2ZJ	Vulnerable; migrate to 12.3(4)T13 or later
12.2ZL	Vulnerable; contact TAC
12.2ZN	Vulnerable; migrate to 12.3(4)T13 or later
12.2ZP	Vulnerable; migrate to 12.4(8) or later
Affected	
12.3-Based	Rebuild Maintenance
Release	

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

12.3	12.3(10f)	12.3(19)
12.3B	Vulnerable; migrate to 12.3(11)T11 or later	
12.3BC	12.3(13a)BC6	
12.3(17a)BC2		
12.3BW	Vulnerable; migrate to 13.3(11)T11 or later	
12.3JA	12.3(8)JA2	
12.3JEA	All 12.3JEA releases are fixed	
12.3JEB	All 12.3JEB releases are fixed	
12.3JK	12.3(2)JK2	
12.3JX	12.3(7)JX4 12.3(11)JX	
12.3(4)T13		
12.3T	12.3(11)T11	
12.3TPC	Vulnerable; contact TAC	
12.3XA	Vulnerable; contact TAC	
12.3XB	Vulnerable; migrate to 12.3(11)T11 or later	
12.3XC	Vulnerable; contact TAC	
12.3XD	Vulnerable; migrate to 12.3(11)T11 or later	
12.3XE	Vulnerable; contact TAC	
12.3XF	Vulnerable; migrate to 12.3(11)T11 or later	
12.3XG	Vulnerable; contact TAC	
12.3XH	Vulnerable; migrate to 12.3(11)T11 or later	
12.3XI	12.3(7)XI8	
12.3XJ	Vulnerable; migrate to 12.3(14)YX2 or later	
12.3XK	Vulnerable; migrate to 12.4(8) or later	
12.3XQ	Vulnerable; migrate to 12.4(8) or later	

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

12.3XR Vulnerable; contact TAC

12.3XS Vulnerable; migrate to 12.4(8) or later

12.3XU Vulnerable; migrate to 12.4(2)T5 or later

12.3XW Vulnerable; migrate to 12.3(14)YX2 or later

12.3XX Vulnerable; migrate to 12.4(8) or later

12.3XY Vulnerable; migrate to 12.4(8) or later

12.3YA Vulnerable; contact TAC

12.3YD Vulnerable; migrate to 12.4(2)T5 or later

12.3YF Vulnerable; migrate to 12.3(14)YX2 or later

12.3YG Vulnerable; migrate to 12.4(2)T5 or later

12.3YH Vulnerable; migrate to 12.4(2)T5 or later

12.3YI Vulnerable; migrate to 12.4(2)T5 or later

12.3YJ Vulnerable; migrate to 12.3(14)YQ8 or later

12.3YK Vulnerable; migrate to 12.4(4)T4 or later

12.3YM 12.3(14)YM8

12.3YQ 12.3(14)YQ8

12.3YS Vulnerable; migrate to 12.4(4)T4 or later

12.3YT Vulnerable; migrate to 12.4(4)T4 or later

12.3YU Vulnerable; contact TAC

12.3YX 12.3(14)YX2

12.3YZ 12.3(11)YZ1

Affected
12.4-Based Rebuild Maintenance
Release

12.4(3e)
12.4 -----
12.4(7b) 12.4(8)

12.4MR 12.4(6)MR1

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

12.4SW	All 12.4SW releases are fixed
12.4(2)T5	
12.4T	12.4(4)T4
12.4(6)T3	12.4(9)T
12.4XA	Vulnerable; migrate to 12.4(6)T3
12.4XB	Vulnerable; contact TAC
12.4XC	12.4(4)XC3
12.4XD	12.4(4)XD4
12.4XE	All 12.4XE releases are fixed
12.4XG	All 12.4XG releases are fixed
12.4XJ	All 12.4XJ releases are fixed
12.4XP	All 12.4XP releases are fixed
12.4XT	All 12.4XT releases are fixed

Workarounds

=====

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

<http://www.cisco.com/warp/public/707/cisco-air-20070124-crafted-tcp.shtml>

Note: Configuring VTY access-class filters is not an effective mitigation strategy for this vulnerability.

Infrastructure ACLs (iACL)

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 ACL example shown below should be included as part of the deployed infrastructure access-list which

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

will protect all devices with IP addresses in the infrastructure IP address range.

A sample access list for devices running Cisco IOS is below:

```
!---- Permit TCP services from trust hosts destined  
!---- to infrastructure addresses.
```

```
access-list 150 permit tcp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK
```

```
!---- Deny TCP packets from all other sources destined to infrastructure addresses.
```

```
access-list 150 deny tcp any INFRASTRUCTURE_ADDRESSES MASK
```

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

```
access-list 150 permit IP any any
```

```
interface serial 2/0  
ip access-group 150 in
```

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/warp/public/707/iacl.html>

Receive ACLs (rACL)

+-----

For distributed platforms, Receive ACLs may be an option starting in Cisco IOS Software Versions 12.0(21)S2 for the 12000 (GSR), 12.0(24)S for the 7500, and 12.0(31)S for the 10720. The Receive ACL protects the device from harmful traffic before the traffic can impact the route processor. Receive ACLs are designed to only protect the device on which it is configured. On the 12000, transit traffic is never affected by a receive ACL. Because of this, the destination IP address "any" used in the example ACL entries below only refer to the router's own physical or virtual IP addresses. On the 7500 and 10720, transit traffic with IP options set will be subject to the Receive ACL and permitted or denied accordingly. Receive 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 "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>

The following is the receive path ACL written to permit this type of traffic from trusted hosts:

```
!---- Permit tcp services from trusted hosts allowed to the RP.
access-list 151 permit tcp TRUSTED_ADDRESSES MASK any
!---- Deny tcp services from all other sources to the RP.
access-list 151 deny tcp any any
!---- Permit all other traffic to the RP.
access-list 151 permit ip any any
!---- Apply this access list to the 'receive' path.
ip receive access-list 151
```

Control Plane Policing (CoPP)

+-----

The Control Plane Policing (CoPP) feature may be used to mitigate this vulnerability. In the following example, only TCP traffic from trusted hosts and with 'receive' destination IP addresses is permitted to reach the route processor (RP). All other 'transit' IP traffic is unaffected.

It should be noted that dropping traffic from unknown or untrusted IP addresses may affect hosts with dynamically assigned IP addresses from connecting to the Cisco IOS device.

```
access-list 152 deny tcp TRUSTED_ADDRESSES MASK any
access-list 152 permit tcp any any
access-list 152 deny ip any any
!
class-map match-all permit-tcp-class
match access-group 152
!
!
policy-map permit-tcp-policy
class permit-tcp-class
drop
!
control-plane
service-policy input permit-tcp-policy
```

In the above CoPP example, the ACL entries that match the 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 are not affected by the policy-map drop function.

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

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

```
policy-map permit-tcp-policy
class class permit-tcp-class
police 32000 1500 1500 conform-action drop exceed-action drop
```

CoPP is available in Cisco IOS release trains 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T.

Additional information on the configuration and use of the CoPP feature can be found at the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_white_paper09186a0080211f39.shtml

Anti-spoofing

+-----

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

http://www.cisco.com/en/US/partner/products/ps6441/products_command_reference_chapter09186a00804ae49f.html#

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

```
router(config)# ip cef
router(config)# interface interface #
router(config-if)# ip verify unicast source reachable-via rx
```

BGP and BTSH/GTSM

+-----

Depending on your release of software, it may be possible to protect your BGP sessions from this memory leak. With the introduction of CSCee73956, Cisco IOS has improved support for BTSH (BGP TTL Security Hack) to reduce, if not eliminate a risk of a memory leak due to this vulnerability. This functionality is also known as GTSM (Generalized TTL Security Mechanism) and documented in RFC 3682. This section refers to GTSM as applied to eBGP sessions only.

Releases of Cisco IOS that contain CSCee73956 are protected from this attack against the BGP port (TCP port 179) only. Other ports should be protected accordingly.

BTSH is not supported for iBGP sessions. BTSH was first introduced in

[VulnWatch] Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

Cisco IOS in 12.0(27)S, 12.3(7)T and 12.2(25)S. Note that the BTSH feature prior to CSCee73956 will not protect against this vulnerability.

For more information on BTSH, please see:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gt_btsh.htm

Obtaining Fixed Software

=====

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. 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