

Cisco Security Advisory: Crafted ICMP Messages Can Cause Denial of Service

Advisory ID: cisco-sa-20050412-icmp

<http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>

Revision 1.3

Last Updated 2005 April 28 2230 UTC (GMT)


For Public Release 2005 April 12 1200 UTC (GMT)

Please provide your **feedback** on this document.

Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Impact](#)
- [Software Versions and Fixes](#)
- [Workarounds](#)
- [Obtaining Fixed Software](#)
- [Exploitation and Public Announcements](#)
- [Status of This Notice: FINAL](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

Summary

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" ([draft-gont-tcpm-icmp-attacks-03.txt](#) ).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:


1. Attacks that use ICMP "hard" error messages
2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP "source quench" messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are [workarounds](#) available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the [National Infrastructure Security Coordination Centre](#)  (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.cpni.gov.uk/Products/alerts/1053.aspx>.

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

☐ **Affected Products**

This section provides details on affected products.

☐ **Vulnerable Products**

Cisco IOS

Cisco products that run Cisco IOS® and that have PMTUD enabled, either by default or because they have been explicitly configured to do PMTUD, are affected. All versions of IOS are impacted. The severity of the exposure depends upon the protocols and applications that rely on specific ICMP messages to perform PMTUD. IOS is not vulnerable to attacks that make use of ICMP "hard" error or "source quench" messages.

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." The image name will be displayed between parentheses shortly after this identification (possibly in the next line), 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 12.2(15)T14 with an installed image name of C806-K9OSY6-M:

```
gw>show version
Cisco Internetwork Operating System Software
IOS (tm) C806 Software (C806-K9OSY6-M), Version 12.2(15)T14, RELEASE SOFT
[...]
```

The following protocols make use of PMTUD and if enabled in the network may cause IOS devices to be vulnerable to PMTUD attacks.

- **Transmission Control Protocol over Internet Protocol (IP) Version 4:** if an IOS device establishes TCP sessions with other devices, for example, to speak Border Gateway Protocol (BGP) with other peers, it may be vulnerable to crafted ICMP "fragmentation needed and DF bit set" error messages if PMTUD is enabled. PMTUD is *disabled by default* for TCP in IOS. PMTUD is enabled if the command **ip tcp path-mtu-discovery** is present in the device configuration.
- **Transmission Control Protocol over Internet Protocol Version 6 (IPv6):** PMTUD is enabled by default for IPV6; therefore, devices configured for IPv6 are vulnerable to PMTUD attacks if they are running services that rely on TCP, like BGP. If the device is just forwarding IPv6 traffic, i.e., it does not establish TCP sessions with other hosts, then it is not affected.
- **IP Security (IPSec):** when an IOS device is configured to use IPSec, PMTUD is *enabled by default*, and therefore, the device may be affected by the PMTUD attack described in this document. An IOS device is configured for IPSec if either **crypto map** or **tunnel protection** is applied to an interface. For example:

```
crypto ipsec profile IPSEC_PROFILE
[...]
!
crypto map MYMAP 1 ipsec-isakmp
[...]
!
interface Tunnel0
 tunnel protection ipsec profile IPSEC_PROFILE
[...]
!
interface Ethernet1
 crypto map MYMAP
[...]
```

- **Generic Routing Encapsulation (GRE) and IPinIP:** devices configured to use these tunneling protocols are vulnerable to crafted ICMP "fragmentation needed and DF bit set" messages if PMTUD is enabled. PMTUD is *disabled by default* for these two protocols. The device is vulnerable if the command **tunnel path-mtu-discovery** is present in the configuration.
- **Layer 2 Tunneling Protocol Version 2 (L2TP) and Layer 2 Tunneling Protocol Version 3 (L2TPv3):** devices configured to use these tunneling protocols are vulnerable to crafted ICMP "fragmentation needed and DF bit set" messages if PMTUD is enabled. PMTUD is *disabled by default* for these protocols. A device running L2TP is vulnerable if the command **ip pmtu** appears in the device's configuration.

Note: L2TP (version 2) and L2TPv3 (version 3) are two different and independent protocols. Both are affected, but throughout the rest of this document we will refer to them as one since they are affected in the same manner.


In addition to IOS-based routers, the following devices also run Cisco IOS or software based on Cisco IOS and *are* therefore vulnerable:

- The Catalyst 4000 and 6000 switches when running IOS in either hybrid (Supervisor Engine running CatOS and Multilayer Switch Feature Card running IOS) or native mode (Supervisor Engine running IOS.)
- Cisco Aironet Wireless LAN Access Points and Bridges.
- Catalyst 2900XL, 2900XL-LRE, 3500XL, 2940, 2950, 2950-LRE, 2955, and 2970 series switches.
- Catalyst 2948G-L3, 3550, 3560, 3750, and 3750-ME series switches.
- The Communication Media Module (CMM)
- Cisco Optical Network Solutions (ONS) products: the ML and SL blades in the ONS 15454, and the ONS 15530/15540.
- Cisco DistributedDirector.


Non-IOS Products

The following non-IOS-based products are also vulnerable:

- Cisco CRS-1: the CRS-1 runs IOS XR, which is vulnerable to PMTUD attacks and to attacks that use ICMP "hard" error messages if the CRS-1 establishes TCP sessions with other devices in applications like BGP. PMTUD is *disabled by default* in IOS XR. PMTUD is enabled if the command **tcp path-mtu-discovery** is present in the device configuration. Use the **show version** command to obtain the version of the running IOS XR software.
- Cisco PIX Security Appliance is vulnerable to PMTUD attacks if it is configured to use IPsec. The only traffic that is affected is traffic going through the particular IPsec tunnel that has been attacked. IPsec *is not enabled* by default on the Cisco PIX Security Appliance. The Cisco PIX Security Appliance is using IPsec if the device configuration shows a crypto map applied to an interface through the command **crypto map <crypto map name> interface <interface name>**. The **show version** command can be used to determine the running version of the Cisco PIX Security Appliance software. Please note that version 7.0 and later of the PIX Security Appliance software is not affected by these vulnerabilities.
- Cisco IP Phones
 - 7940/7960 with Skinny Client Control Protocol (SCCP) firmware.
 - 7940/7960 with Session Initiation Protocol (SIP) firmware.
 - 7970 with Skinny Client Control Protocol firmware (vulnerable only to crafted ICMP "hard" error messages)The version of the firmware running on your Cisco IP Phone can be found by pressing the "Settings" button of your phone and selecting the "Status" menu options.
- Cisco Catalyst 6000 Voice E1/T1 and Services Module (WS-X6608-E1 and WS-X6608-T1) running Digital PRI Gateway, Conference Bridge, or Transcoder/MTP firmware; and Cisco 6000 FXS Analog Interface Module (WS-X6624-FXS) are vulnerable to crafted ICMP "hard" errors, as well as to crafted ICMP "source quench" messages. To obtain the version of the 6608 and 6624 firmware, log in to your Catalyst 6500 series switch and issue the **show version** command.
- Cisco 11000 and 11500 Content Services Switches (CSS).
- Global Site Selector (GSS).
- Cisco ONS products: ONS 15302 and ONS 15305.
- Cisco MDS 9000 Series Multilayer Switches.

- Cisco VPN 5000 concentrator.
- Cisco MGX-8250 (PXM-1 based) and MGX-8850 (PXM-1E and PXM-45 based) - vulnerable on the control plane only; switching services are not impacted.
- Cisco Content Switching Module (CSM) - vulnerable control plane only; switching services are not impacted.
- Microsoft Security Bulletin [MS05-019](#)  states that Microsoft Windows is vulnerable to PMTUD attacks and to attacks based on ICMP "hard" error messages. The following voice and IP communication products are shipped with, and run on top of, the Microsoft Windows operating system. The customization of Microsoft Windows made by Cisco and included with these products has PMTUD disabled by default starting with release 2000.2.5 (releases 2000.2.4 and before use the Microsoft default which is to enable PMTUD.) These products are vulnerable to attacks based on ICMP "hard" errors as well as to PMTUD attacks (if PMTUD is enabled):

- Cisco Call Manager
- Cisco Conference Connection
- Cisco Customer Voice Portal (previously Internet Service Node)
- Cisco Emergency Responder
- Cisco IP Call Center Express
- Cisco IP Interactive Voice Response
- Cisco IP Queue Manager
- Cisco MeetingPlace
- Cisco Personal Assistant

- The following products use non-Cisco-customized versions of Microsoft Windows. PMTUD is enabled by default on Microsoft Windows, so these products may be vulnerable to PMTUD attacks if this default setting has not been changed, and are vulnerable to attacks based on ICMP "hard" error messages, as described in Microsoft Security Bulletin [MS05-019](#) :

- Cisco Agent Desktop
- Cisco Intelligent Contact Management Product Family
- Cisco IP Contact Center Enterprise Edition
- Cisco IP Contact Center Product Family
- Cisco Remote Monitoring Suite Option
- Cisco Support Tools
- Cisco Unity

To verify whether PMTUD is enabled in the version of Microsoft Windows used by your Cisco product, please check the value of the following registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\
Parameters\EnablePMTUDiscovery
```

If this registry key is present then PMTUD is enabled or disabled based on the value of the key. If they key is not present, PMTUD is enabled.

- The Cisco Secure ACS Solution Engine, also known as the Cisco Secure ACS Appliance, is based on Microsoft Windows, and therefore is vulnerable to PMTUD attacks and to attacks based on ICMP "hard" error messages. However, recent versions of the ACS Solution Engine ship with Cisco Security Agent (CSA), which is configured to block all incoming ICMP messages. Under this situation the Cisco Secure ACS Solution Engine is not vulnerable to any of the attacks described in this document.

To determine if you have CSA installed and working, you can try sending ICMP echo

requests (ping) to the ACS appliance. If ICMP echo replies are received CSA is not enabled or installed.

To check to see if CSA is available go to "System Configuration:Upgrade Appliance" and see what version is installed. Then go to "System Configuration:Appliance Configuration" and see if CSA is enabled.

☐ **Products Confirmed Not Vulnerable**

The following products are not vulnerable:

- Cisco Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series and Cisco 7600 Series.
- Cisco Guard and Cisco Traffic Anomaly Detector Denial of Service mitigation appliances.
- Catalyst Switches. The following Catalyst switches *do not* run Cisco IOS and therefore are *not affected* by the vulnerabilities described in this document:
 - 1200
 - 1700
 - 1900
 - 2100
 - 28xx
 - 2948G-GE-TX
 - 2900, 2902, 2926T and 2926G
 - 3000, 3100, 3200
 - 3900
 - 5000
 - The Catalyst 4000 and 6000 switches can run CatOS or IOS. When running CatOS, they *are not* vulnerable unless a Multilayer Switch Feature Card (MSFC) is present (since the MSFC runs IOS.) When running IOS, they are vulnerable as described above in the [Vulnerable Products](#) section.
- Cisco ONS products: ONS 15327 Metro Edge Optical Transport Platform, ONS 15454 Optical Transport Platform (MSPP and MSTP), ONS 15531/15532 T31 OMDS Metro WDM System, ONS 15216 EDFA3/EDFA2/OADM, ONS 15310 CL.
- Cisco IP Phones
 - ATA 186/188
 - 7910
 - 7902/05
 - 7912
 - 7920
- Cisco VG248 Analog Phone Gateway
- Cisco VPN 3000 Series Concentrators, VPN 3002 Hardware Clients, and the VPN Software Client (please note that the VPN Software Client itself is not vulnerable but the operating system the VPN clients runs on *may* be vulnerable. Please check with your operating system vendor.)
- Cisco BTS 10200 Softswitch
- Content Engines, Content Routers, and Content Distribution Managers running Cisco Application and Content Networking System (ACNS) software.
- Cisco LocalDirector

Summary of Vulnerable Products

The following table summarizes how Cisco products are affected by the vulnerabilities described in this document:

Product	Hard Error	PMTUD	Source Quench
IOS	Not affected	Affected	Not affected
IOS XR	Affected	Affected	Not affected
IP Phones	Affected	Affected	Affected
Cisco PIX Security Appliance	Not affected	Affected	Not affected
Catalyst 6608 and 6624	Affected	Not affected	Affected
Cisco 11000 and 11500	Not affected	Not affected	Affected
Cisco GSS	Not affected	Not affected	Affected
MDS 9000	Not affected	Affected	Affected
Cisco VPN 5000 Concentrator	Not affected	Affected	Not affected
Some ONS products	Not affected	Affected	Not affected
Cisco MGX-8250 and MGX-8850	Affected	Affected	Affected
Cisco Content Switching Module	Not affected	Not affected	Affected
Voice and IP Communication Products Using Cisco-Customized Microsoft Windows	Affected	Affected	Not affected
Cisco ACS Solution Engine	Affected	Affected	Not affected

Please refer to the [Details](#) section for additional information since within one product family different models may be affected differently.

Summary of Vulnerable Products

The following table summarizes how Cisco products are affected by the vulnerabilities described in this document:

Product	Hard Error	PMTUD	Source Quench
IOS	Not affected	Affected	Not affected
IOS XR	Affected	Affected	Not affected
IP Phones	Affected	Affected	Affected
Cisco PIX Security Appliance	Not affected	Affected	Not affected
Catalyst 6608 and 6624	Affected	Not affected	Affected
Cisco 11000 and 11500	Not affected	Not affected	Affected
Cisco GSS	Not affected	Not affected	Affected
MDS 9000	Not affected	Affected	Affected
Cisco VPN 5000 Concentrator	Not affected	Affected	Not affected
Some ONS products	Not affected	Affected	Not affected
Cisco MGX-8250 and MGX-8850	Affected	Affected	Affected
Cisco Content Switching Module	Not affected	Not affected	Affected
Voice and IP Communication Products Using Cisco-Customized Microsoft Windows	Affected	Affected	Not affected
Cisco ACS Solution Engine	Affected	Affected	Not affected

Please refer to the [Details](#) section for additional information since within one product family different models may be affected differently.



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


☐ **Details**

The Internet Control Message Protocol is an integral part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite that is used to report error conditions and provide diagnostic information. ICMP error messages can be generated by both end systems and


intermediate systems, i.e., routers. End systems and intermediate systems react to error messages received via ICMP in different ways depending on the type of error that is being reported. The types of errors that can be reported via ICMP fall into two categories: "soft" errors and "hard" errors.

RFC 1122 ("Requirements for Internet Hosts - Communications Layers" -

<http://www.ietf.org/rfc/rfc1122.txt> ) , defines three "hard" errors ("protocol unreachable", "port unreachable", and "fragmentation needed and Don't Fragment bit set") and five "soft" errors ("network unreachable", "host unreachable", "source route failed", "time exceeded", and "parameter problem".) "Source quench" is another ICMP error message that can be generated by Internet hosts, and while [RFC 1122](#)  does not clearly classify it as "soft" or "hard", it should be considered as a soft error because of the way this message type should be handled by hosts that receive it: hosts should cut back for a period of time the rate at which they are sending data to the host that generated the ICMP "source quench" message, and then gradually increase the transmission rate again.


It is important to note that the "fragmentation needed and Don't Fragment bit set" (type 3, code 4) message is used by an important mechanism called Path MTU Discovery, documented in RFC 1191 ("Path MTU discovery" - <http://www.ietf.org/rfc/rfc1191.txt> ). PMTUD allows some protocols of the TCP/IP protocol suite to dynamically find the MTU of a path so IP fragmentation is minimized and bandwidth can be used more efficiently. This mechanism is not mandatory for Internet hosts, but those that implement it need to treat ICMP "fragmentation needed and DF bit set" messages as "soft" errors. A good reference to understand how IP fragmentation works and the role that PMTUD plays in reducing fragmentation is the Cisco white paper "IP Fragmentation and PMTUD", available at http://www.cisco.com/en/US/tech/tk827/tk369/technologies_white_paper09186a00800d6979.shtml.

Making a distinction between the types of errors ("soft" versus "hard") that can be reported via ICMP is important because it dictates how Internet hosts will respond to them. In general, connection-oriented protocols like TCP should abort an existing connection in response to an ICMP "hard" error message, and Internet hosts should try to correct the error condition that elicited the receipt of an ICMP "soft" error message.

An IETF Internet Draft entitled "ICMP Attacks Against TCP" ([draft-gont-tcpm-icmp-attacks-03.txt](#) ) that describes how the ICMP protocol can be used to perform a number of Denial of Service attacks against the TCP protocol has been made publicly available. These attacks require knowledge of the IP addresses and ports (in the case of TCP) that two Internet hosts are using to communicate with each other and can cause connection resets and reduction of throughput in existing connections.

Note: these attacks only affect sessions terminating or originating on a device itself, not transit traffic; i.e., traffic that passes through a device, but is destined elsewhere is not affected.

Attacks Based on Crafted Hard ICMP Error Messages

Upon receipt of a "hard" ICMP error message, an Internet host must abort the connection with the host to which the ICMP error message applies. This host is not necessarily the system that generated the ICMP message, but it is uniquely identified through the IP header and transport protocol data embedded in the ICMP payload. The reason for this is that "hard" errors represent serious network problems for which there is not a possibility for recovery. Crafted "hard" ICMP error messages could cause an Internet host to incorrectly abort an existing connection when in reality there are no network problems. This type of attack is classified as a "blind connection-reset" attack in the Internet Draft [draft-gont-tcpm-icmp-attacks-03.txt](#) .

PMTUD Attacks

Crafted "fragmentation needed and DF bit set" ICMP messages can be used to set a connection's Path MTU to a very low, impractical value, if an Internet host is performing PMTUD. This value can cause higher layer protocols to start timing out because of a very low throughput, even though the connection is still in the established state. This type of attack is classified as a "throughput-reduction" attack in the Internet Draft [draft-gont-tcpm-icmp-attacks-03.txt](#).

Per the PMTUD algorithm described in [RFC 1191](#), implementations must "age" cached MTU values, which means that the MTU will go back to its optimum size, a process that can take up to 10 minutes ([RFC 1191](#) suggests 10 minutes, but this is not a requirement and therefore it is implementation-dependent.) Please note, however, that if an attacker continues to send crafted ICMP "fragmentation needed and DF bit set" messages to a vulnerable host, the cached MTU will never age, causing a continuous denial-of-service condition.

As mentioned before, the ICMP "fragmentation needed and DF bit set" message is considered a "hard" error per [RFC 1122](#) if the Internet host receiving it is not performing PMTUD. This means that a PMTUD attack also has the potential to cause a connection reset.

For protocols that make use of a "transport layer" MTU to minimize the risk of fragmentation, like TCP and its Maximum Segment Size (MSS) variable, a good way to determine if a connection is suffering from a successful attack is to monitor the value of this "transport layer" MTU - an unreasonably low value may indicate that an attack has been performed. An example of how to do this in Cisco IOS will be provided later in this document.

Note: several common protocols make use of TCP, and therefore may be affected by PMTUD attacks. Some examples include BGP, the Hyper Text Transfer Protocol (HTTP - used in the World Wide Web), the Simple Mail Transfer Protocol (SMTP - used for transferring electronic mail), and Secure Shell (SSH). Some protocols in the IBM suite like Data-Link Switching (DLSw), Serial Tunneling (STUN), and Block Serial Tunneling (BSTUN) can be configured to use TCP as their transport protocol. The Domain Name System (DNS) normally uses User Datagram Protocol (UDP) but in some situations (large zone transfers, for example) it also uses TCP.

Attacks Based on Crafted Source Quench ICMP Messages

As mentioned before, Internet hosts are supposed to cut back the rate at which they send data to another host that generated an ICMP "source quench" message. While the actual response to an ICMP "source quench" message varies by TCP/IP implementation and by the transport layer protocol in use, in general, hosts receiving an ICMP "source quench" message should trigger a congestion avoidance algorithm.

In the case of a host using TCP to communicate with another, if an ICMP "source quench" message is received the recommended procedure per [RFC 1122](#) is to trigger a "slow start", as if a retransmission timeout had occurred. RFC 2001 ("TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms" - <http://www.ietf.org/rfc/rfc2001.txt>) describes the "slow start" and "congestion avoidance" algorithms used in modern implementations of TCP and states that in practice, the "slow start" and "congestion avoidance" algorithms are implemented together.

The lower rate at which the sending host transmits data allows the host that generated the ICMP "source quench" message to process and empty its receive buffers.

Crafted "source quench" ICMP messages can be used to decrease the rate at which a host is sending data. While over time, as long as no additional Source Quench messages are received, the window size will increase to a reasonable value, a crafted "source quench" message can potentially reduce communication efficiency significantly. If an attacker succeeds in periodic transmission of crafted ICMP "source quench" messages to a vulnerable device, a prolonged degradation of service for that connection may occur.

This type of attack is classified as a "throughput-reduction" attack in the Internet Draft [draft-gont-tcpm-icmp-attacks-03.txt](#).

How Cisco Products Are Affected

Different Cisco products are affected in different ways to the ICMP attacks described in this document. In some cases, some products are affected when specific configurations or network protocols are in use. What follows is a description of how vulnerable products are affected and under what configurations. Information about specific Cisco bug IDs for each product is presented.

Cisco IOS

Cisco IOS is not vulnerable to attacks that make use of ICMP "hard" error messages because IOS checks whether a connection is in the "established" state, and takes action only for connections in the "non-established" state.


In addition, IOS does not process ICMP "source quench" messages and therefore, is not vulnerable to attacks that are based on crafting this type of message.

IOS is vulnerable to PMTUD attacks as described in the [Vulnerable Products](#) section. This means that an attacker could change the Path MTU by crafting an ICMP "fragmentation needed and DF bit set" message ("packet too big" message in the case of IPv6.) The following list provides the Cisco bug IDs for the PMTUD vulnerabilities in different protocols in IOS:

- **All protocols that make use of PMTUD:** [CSCef60659](#) ([registered](#) customers only) -- More stringent checks required for ICMP unreachable.
- **Transmission Control Protocol over Internet Protocol Version 4:** [CSCed78149](#) ([registered](#) customers only) -- TCP connections over IP version 4 doing PMTUD are vulnerable to crafted ICMP packets.

A good way to verify whether a connection is suffering from the effects of a PMTUD attack is by looking at the MSS value of the connection. For BGP sessions the command **show ip bgp neighbors | include data segment** will display the MSS (denoted as max data segment), as in the following example:

```
Router#show ip bgp neighbors | include data segment
Datagrams (max data segment is 1460 bytes):
Router#
```


The official minimum MTU is 68 bytes, although in today's Internet a MSS less than 576 bytes should be considered suspicious. Section 7 of [RFC 1191](#)  contains a list of common

MTU values used on the Internet.

For other TCP connections, the Transmission Control Block (TCB) of a specific connection must be determined using the command **show tcp brief**, and then this TCB must be used in the command **show tcp tcb <TCB identified with show tcp brief> | include data segment**, which will display the MSS (denoted again as `max data segment`):

```
Router#show tcp brief
TCB          Local Address          Foreign Address        (state)
00E97148     192.168.100.1.23      192.168.100.1.11002   TIMEWAIT
00E97A78     192.168.100.1.23      192.168.100.1.11003   ESTAB
00E975E0     192.168.100.1.11003   192.168.100.1.23     ESTAB
Router#show tcp tcb 0x00E975E0 | include data segment
Datagrams (max data segment is 1474 bytes):
Router#
```

Please note that this technique can also be used for TCP over IPv6.

- **Transmission Control Protocol over Internet Protocol Version 6:** [CSCef61610](#) ([registered customers only](#)) -- Incorrect handling of ICMPv6 messages can cause TCP performance problems.
- **IPSec:** [CSCsa59600](#) ([registered customers only](#)) -- IOS IPSec connections may be vulnerable to crafted ICMP packets which may cause IPSec to use very small PMTU values for a given flow. After the PMTU has been decreased by a crafted ICMP "fragmentation needed and DF bit set" message, if no additional ICMP "fragmentation needed and DF bit set" messages are received, the learned MTU will be active for 10 minutes, after which the PMTU is restored to the first-hop data-link MTU, per [RFC 1191](#) .

A way to verify whether an IPSec tunnel is suffering from the effects of a PMTUD attack is by running the command **show crypto ipsec sa | include mtu**, as in the following example:

```
Router#show crypto ipsec sa | include mtu
  path mtu 1500, media mtu 1500
Router#
```

- **Generic Routing Encapsulation and IPinIP:** [CSCef44699](#) ([registered customers only](#)) -- GRE and IPinIP tunnels may be vulnerable to crafted ICMP packets. A way to verify whether a GRE or IPinIP tunnel is suffering from the effects of a PMTUD attack is by running the command **show interface tunnel <number> | include Path MTU**, as in the following example:

```
Router#show interface tunnel 0 | include Path MTU
  Path MTU Discovery, ager 10 mins, MTU 1476, expires never
```

Please note that in the case of these tunneling protocols, the ICMP error message does not include enough information about the GRE or IPinIP packet that elicited the error to be able to properly authenticate the message. For this reason the Cisco Bug ID [CSCef44699](#) ([registered customers only](#)) adds a new command that allows users to specify the minimum Path MTU they expect to have across their GRE tunnels. The new command is **tunnel path-mtu-discovery min-mtu <minimum MTU>** and is available under tunnel interface configuration mode. When this command is in use, and the device receives an ICMP "fragmentation needed and DF bit set" message that advertises a next-hop Path MTU less than the configured minimum Path MTU, the device will produce a log message similar to the following:

```
%TUN-5-IGNOREICMPMTU Tunnel1 ignoring received ICMP Type 3 Code 4,
```

due to pmtud min-mtu setting

- **Layer 2 Tunneling Protocol Version 2 and Layer 2 Tunneling Protocol Version 3:** for L2TP version 2 the Cisco bug ID is [CSCsa52807](#) ([registered](#) customers only) -- L2TPv2 doing PMTUD vulnerable to spoofed ICMP packets. For L2TP version 3 the bug ID is [CSCef43691](#) ([registered](#) customers only) -- Connections using Layer 2 Tunneling Protocol v3 (L2TPv3) and doing PMTUD discovery may be vulnerable to crafted ICMP packets. A way to verify whether a L2TPv2 session is suffering from the effects of a PMTUD attack is by running the command **show vpdn session all | include Session MTU**, as in the following example:

```
Router#show vpdn session all | include Session MTU
Session MTU is 68 bytes
```

For L2TPv3, a PMTUD attack can be identified by running the command **show l2tun session all | include PMTU**, as in the following example:

```
Router#show l2tun session all | include Session MTU
Session PMTU enabled, path MTU is 68 bytes
Session PMTU enabled, path MTU is 68 bytes
Session PMTU enabled, path MTU is 68 bytes
```

Please note that in the case of L2TPv2, the ICMP error message does not include enough information about the L2TPv2 packet that elicited the error to be able to properly authenticate the message. For this reason, the fix for Cisco Bug ID [CSCsa52807](#) ([registered](#) customers only) adds a new commands that allow users to specify the minimum and maximum Path MTU they expect to have across their L2TPv2 tunnels. The new commands are **vpdn pmtu minimum <minimum MTU>** and **vpdn pmtu maximum <maximum MTU>** and are available under **vpdn-group** configuration mode. When these commands are in use, and the device receives an ICMP "fragmentation needed and DF bit set" message that advertises a next-hop Path MTU outside the minimum and maximum range, the device will produce the following log message:

```
%VPDN-5-IGNOREICMPMTU Ignoring received ICMP Type 3 Code 4,
due to pmtu min or max setting
```

IOS XR

IOS XR is vulnerable to attacks based on ICMP "hard" error messages, as well as to PMTUD attacks. The Cisco Bug ID that documents this vulnerability is [CSCef45332](#) ([registered](#) customers only) -- CRS-1 connections may be vulnerable to crafted ICMP packets. IOS XR does not process ICMP "source quench" messages, so it is not vulnerable to attacks based on this type of message.


Cisco IP Phones


Different models of Cisco IP Phones are vulnerable to attacks based on ICMP "hard" error messages, ICMP "source quench" messages, and/or PMTUD attacks.

- [CSCef46728](#) ([registered](#) customers only) -- 7940/7960 IP Phone with SCCP firmware may be susceptible to crafted ICMP "hard" error messages.
- [CSCef54947](#) ([registered](#) customers only) -- 7970 IP Phone with SCCP firmware may be susceptible to crafted ICMP "hard" error messages.

- [CSCef54204](#) ([registered](#) customers only) -- 7940/7960 IP Phone with SIP firmware may be vulnerable to crafted ICMP "source quench" error messages. Please note that a 7940/7960 IP Phone with SIP firmware does not support TCP for signaling, so only telnet sessions into the phone (for management) and short-lived HTTP sessions from the phone (to servers providing directory services, for example) are affected by this vulnerability.
- [CSCef54206](#) ([registered](#) customers only) -- 7940/7960 IP Phone with SIP firmware may be vulnerable to crafted ICMP "hard" error messages. Please note that a 7940/7960 IP Phone with SIP firmware does not support TCP for signaling, so only telnet sessions into the phone (for management) and short-lived HTTP sessions from the phone (to servers providing directory services, for example) are affected by this vulnerability.

Cisco PIX Security Appliance

A PIX Security Appliance with IPSec configured will actively participate in PMTUD per [RFC 1191](#)  and RFC 2401 ("Security Architecture for the Internet Protocol" -

<http://www.ietf.org/rfc/rfc2401.txt> ) This means that the PIX Security Appliance can dynamically discover and adjust its path MTU for a given IPSec flow when it receives an ICMP "fragmentation needed and DF bit set" message.

Under this scenario, the PIX Security Appliance is also vulnerable to crafted ICMP type 3 code 4 messages that try to set the path MTU to a very low value. This vulnerability is documented in the Cisco Bug ID [CSCef57566](#) ([registered](#) customers only) -- A PIX Security Appliance with IPSec configured can be susceptible to crafted ICMP packets suggesting a very small PMTU for a path or a Security Association. This symptom is observed when IPSec is configured for PMTUD, which is turned on automatically when IPSec is configured on the PIX Security Appliance.

Catalyst 6608 and 6624

The Cisco Catalyst 6000 Voice E1/T1 and Services Module (WS-X6608-E1 and WS-X6608-T1) running Digital PRI Gateway, Conference Bridge, or Transcoder/MTP firmware Cisco 6000 FXS Analog Interface Module (WS-X6624-FXS) are vulnerable to attacks based on ICMP "hard" error and "source quench" messages. The Cisco Bug ID that documents these vulnerabilities is [CSCsa60692](#) ([registered](#) customers only) -- ICMP Hard error handling.

Cisco 11000 and 11500 Content Services Switches

The Cisco 11000 and 11500 Content Services Switches are vulnerable to attacks based on ICMP "source quench" messages on the *management* port; they are not vulnerable on the network ports. The CSS does not perform PMTUD and therefore is not vulnerable to PMTUD attacks. The Cisco Bug ID that documents the vulnerability to ICMP "source quench" messages is [CSCeh45454](#) ([registered](#) customers only) -- ICMP error packet attacks against TCP.

Cisco Global Site Selector

The Cisco Global Site Selector version 1.2 and earlier is vulnerable to attacks based on ICMP "source quench" messages. It is not vulnerable to attacks based on ICMP "hard" error messages or to PMTUD attacks. The Cisco Bug ID that documents the vulnerability to ICMP "source quench" messages is [CSCeh20083](#) ([registered](#) customers only) -- ICMP error packet attacks against TCP.

Cisco MDS 9000 Series Multilayer Switches

The Cisco MDS 9000 Series Multilayer Switch is vulnerable to PMTUD and "source quench" attacks. The Cisco Bug ID that documents this vulnerability is [CSCeh04183](#) ([registered](#) customers only) -- ICMP attacks against TCP.

Cisco ONS Products

The affected Cisco ONS products are vulnerable to PMTUD attacks only.

VPN 5000 Concentrator

The VPN 5000 concentrator is vulnerable to PMTUD attacks. ICMP "source quench" messages are only processed to keep message counts, but not for avoiding congestion. Therefore, this device is not vulnerable to attacks based on this type of messages. The Cisco Bug ID that documents the PMTUD vulnerability is [CSCeh59823](#) ([registered](#) customers only) -- ICMP 3/4 messages may affect IPsec sessions.


Cisco MGX-8250 and MGX-8850

The Cisco MGX1 (PXM1) and MGX2 (PXM45s, PXM1E) are vulnerable to ICMP "source quench" attacks, PMTUD attacks, and ICMP "hard" error attacks on the *management* side. Please note that this affects management TCP connections (telnet, SSH) and not switching services. The Cisco Bug IDs that track these vulnerabilities are [CSCeh65337](#) ([registered](#) customers only) for the Cisco MGX1 and [CSCeh63449](#) ([registered](#) customers only) for the Cisco MGX2.

Cisco Content Switching Module

The Cisco Content Switching Module is vulnerable to ICMP "source quench" attacks on TCP-based management connections to the device. Traffic going through the device is not impacted.

Cisco Products That Include Versions of Microsoft Windows

Voice and IP communication products that use a Cisco-customized version of Microsoft Windows, and the ACS Solution Engine, which also includes a version of Microsoft Windows, are vulnerable to PMTUD attacks and to attacks based on ICMP "hard" error messages. For details about these vulnerabilities in Microsoft Windows, please refer to Microsoft Security Bulletin [MS05-019](#) .

There is no Cisco Bug ID to track these vulnerabilities in the voice and IP communication products. For the ACS Solution Engine, the Cisco Bug ID used to track these vulnerabilities is [CSCeh62307](#) ([registered](#) customers only) .

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

☐ Impact

Successful exploitation of attacks using crafted ICMP "hard" error messages may result in connections being dropped.

Successful exploitation of attacks based on "fragmentation needed and DF bit set" (or PMTUD attacks) and ICMP "source quench" error messages may result in connections being throttled to very

low throughput. While throughput is low, the output buffer of a sending host could overflow or packets could be dropped or be unnecessarily fragmented, which may affect applications and communication efficiency. Accordingly, crafted ICMP packets could interfere with network protocols, such as the Border Gateway Protocol, Label Distribution Protocol (LDP) and DLSw.

In addition to causing low throughput, a PMTUD attack can also cause high Central Processing Unit (CPU) utilization and extra memory consumption on the receiving host because the CPU will spend time and memory buffers to reassemble the incoming fragmented packets.

In all cases, these attacks may result in Denial-of-Service conditions. No remote code execution or unauthorized access results from these types of attacks.

For devices that are vulnerable only on the control plane, it is important to note that switching services for traffic traversing the device, i.e. the data plane, are not impacted.

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

☐ Software Versions and Fixes

When considering software upgrades, please also consult http://www.cisco.com/en/US/products/products_security_advisories_listing.html 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") for assistance.

IOS-based Products

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

For further information on the terms "Rebuild" and "Maintenance" please consult the following URL:

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

Due to differences in software availability and in the feature scenarios in which Cisco IOS is vulnerable, the table of first fixed releases has been broken down based on the different vulnerabilities that affect each technology. There are four different groups:

1. **TCPv4:** represents [CSCed78149](#) ([registered](#) customers only) and [CSCef60659](#) ([registered](#) customers only) . The first Cisco Bug ID tracks TCP's vulnerability to PMTUD attacks, and the second

Cisco Bug ID tracks the vulnerability that affects all protocols that make use of PMTUD, with the exception of TCP over IPv6, which is not affected by this vulnerability.

2. **Tunnels:** represents [CSCef60659](#) ([registered](#) customers only) , [CSCef43691](#) ([registered](#) customers only) , [CSCsa61864](#) ([registered](#) customers only) , [CSCsa59600](#) ([registered](#) customers only) , and [CSCef44699](#) ([registered](#) customers only) . These are the Cisco Bug IDs that track vulnerabilities in most of the affected tunneling protocols (GRE, L2TPv3, and IPsec.)
3. **TCPv6:** represents [CSCef61610](#) ([registered](#) customers only) , which is the Cisco Bug ID that tracks TCP's vulnerability to PMTUD attacks when running over IPv6.
4. **L2TPv2:** represents [CSCsa52807](#) ([registered](#) customers only) , which is the Cisco Bug ID that tracks L2TPv2's vulnerability to PMTUD attacks.

Major Release		Availability of Repaired Releases	
Affected 12.0-Based Release		Rebuild	Maintenance
12.0	TCPv4 and Tunnels	12.0(28c)	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0DA	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(12) DA8 or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0DB	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0DC	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(15) BC2f or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0S	TCPv4 and Tunnels	12.0(27)S5, available 23-May-05	12.0(31)S, available 28-Apr-05
		12.0(28)S3, available 25-Apr-05	
		12.0(30)S1	
		12.0(27)S5,	

	TCPv6	available 23-May-05	12.0(31)S, available 28-Apr-05
		12.0(28)S3, available 25-Apr-05	
		12.0(30)S1	
	L2TPv2	Not vulnerable	
12.0SC	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(15) BC2f or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0SL	TCPv4 and Tunnels	Vulnerable; migrate to 12.0S or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0SP	TCPv4 and Tunnels	Vulnerable; migrate to 12.0S or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0ST	TCPv4 and Tunnels	Vulnerable; migrate to 12.0S or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0SX	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Not vulnerable	
12.0SZ	TCPv4 and Tunnels	Vulnerable; migrate to 12.0S or later	
	TCPv6	Vulnerable; migrate to 12.0S or later	
	L2TPv2	Not vulnerable	
	TCPv4	Vulnerable; migrate to 12.1(27) or	

12.0T	and Tunnels	later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0W5	TCPv4 and Tunnels	12.0(25)W5 (27c)
		12.0(28)W5 (31a)
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0WC	TCPv4 and Tunnels	12.0(5)WC12, available 25-July-05
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XA	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XB	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XC	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XD	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XE	TCPv4 and Tunnels	Vulnerable; migrate to 12.1E latest
	TCPv6	Not vulnerable

	L2TPv2	Not vulnerable
12.0XF	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XG	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XH	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XI	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XJ	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XK	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XL	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XM	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later

	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0XN	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0XQ	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0XR	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0XS	TCPv4 and Tunnels	Vulnerable; migrate to 12.1E latest	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0XV	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
Affected 12.1-Based Release		Rebuild	Maintenance
12.1	TCPv4 and Tunnels		12.1(27)
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1AA	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	

12.1AX	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(25)EY or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1AZ	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(22)EA4 or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1DA	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(12)DA8 or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1DB	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1DC	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(15)BC2f or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1E	TCPv4 and Tunnels	12.1(22)E6, available 02-May-05	
		12.1(23)E3, available 02-May-05	
		12.1(26)E1	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1EA	TCPv4 and Tunnels	12.1(22)EA4	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	

12.1EB	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1EC	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(15) BC2f or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1EO	TCPv4 and Tunnels	12.1(19)EO4, available 26-May-05	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1EU	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(20)EU or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1EV	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1EW	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(18) EW3 or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1EX	TCPv4 and Tunnels	Vulnerable; migrate to 12.1E latest	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1EY	TCPv4 and Tunnels	Vulnerable; migrate to 12.1E latest	
	TCPv6	Not vulnerable	

	L2TPv2	Not vulnerable
12.1T	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XA	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XB	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XC	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XD	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XE	TCPv4 and Tunnels	Vulnerable; migrate to 12.1E latest
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XF	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XG	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later

	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XH	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XI	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XJ	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XL	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XM	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XP	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XQ	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
	TCPv4 and	Vulnerable; migrate to 12.3(13) or

12.1XR	Tunnels	later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XT	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XU	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XV	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1YA	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1YB	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1YC	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1YD	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable

12.1YE	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1YF	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1YH	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1YI	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1YJ	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(22) EA4 or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
Affected 12.2-Based Release		Rebuild	Maintenance
12.2	TCPv4 and Tunnels		12.2(28)
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2B	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	

12.2BC	TCPv4 and Tunnels	12.2(15)BC2f	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; contact TAC	
12.2BW	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; migrate to 12.3 or later	
12.2BY	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.2BZ	TCPv4	Vulnerable; migrate to 12.3(7)XI3	
	Tunnels	Vulnerable; migrate to 12.3(7)XI5, available TBD	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; contact TAC	
12.2CX	TCPv4 and Tunnels	12.2(15)BC2f	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; contact TAC	
12.2CY	TCPv4 and Tunnels	12.2(15)BC2f	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; contact TAC	
12.2CZ	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; contact TAC	
	TCPv4 and	12.2(12)DA8	

12.2DA	Tunnels		
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2DD	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2DX	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2EU	TCPv4 and Tunnels		12.2(20)EU
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Not vulnerable	
12.2EW	TCPv4 and Tunnels	12.2(18)EW3	
	TCPv6	Vulnerable; migrate to 12.2S	
	L2TPv2	Not vulnerable	
12.2EWA	TCPv4 and Tunnels	12.2(25)EWA	
	TCPv6	12.2(25)EWA	
	L2TPv2	Not vulnerable	
12.2EX	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(25) SEB or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2EY	TCPv4 and Tunnels	12.2(25)EY	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	

12.2JA	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(4)JA	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2JK	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.2MB	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.2MC	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T	
	TCPv6	Vulnerable; migrate to 12.3(14)T	
	L2TPv2	Vulnerable; migrate to 12.3(14)T	
12.2S	TCPv4 and Tunnels	12.2(14)S13	
		12.2(18)S8	
		12.2(20)S7	
		12.2(25)S3	
	TCPv6	12.2(20)S7	
		12.2(25)S3	
L2TPv2	Not vulnerable		
12.2SE	TCPv4 and Tunnels	12.2(25)SEB	
	TCPv6	12.2(25)SEA vulnerable; migrate to 12.2(25)SEB	
	L2TPv2	Not vulnerable	
12.2SO	TCPv4 and Tunnels	12.2(18)SO1, available 25-Mar-05	
	TCPv6	12.2(18)SO2, available 29-Apr-05	

	L2TPv2	Not vulnerable	
12.2SU	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Not vulnerable	
12.2SV	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(25)S3	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2SW	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2SX	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(17d) SXB7	
	TCPv6	Vulnerable; migrate to 12.2(17d) SXB7	
	L2TPv2	Not vulnerable	
12.2SXA	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(17d) SXB7	
	TCPv6	Vulnerable; migrate to 12.2(17d) SXB7	
	L2TPv2	Not vulnerable	
12.2SXB	TCPv4 and Tunnels	12.2(17d)SXB7	
	TCPv6	12.2(17d)SXB7	
	L2TPv2	Not vulnerable	
12.2SXD	TCPv4 and Tunnels	12.2(18)SXD4	
	TCPv6	12.2(18)SXD4	
	L2TPv2	Not vulnerable	
	TCPv4	Vulnerable; migrate to 12.2(17d)	

12.2SY	and Tunnels	SXB7	
	TCPv6	Vulnerable; migrate to 12.2(17d) SXB7	
	L2TPv2	Not vulnerable	
12.2SZ	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(20)S7	
	TCPv6	Vulnerable; migrate to 12.2(20)S7	
	L2TPv2	Not vulnerable	
12.2T	TCPv4 and Tunnels	12.2(15)T15	
	TCPv6	12.2(15)T15	
	L2TPv2	Vulnerable; contact TAC	
12.2XA	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2XB	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; migrate to 12.3 or later	
12.2XC	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.2XD	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; migrate to 12.3 or later	
12.2XE	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	

	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XF	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(15) BC2f
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; contact TAC
12.2XG	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XH	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XI	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XJ	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XK	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XL	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
	TCPv4 and	Vulnerable; migrate to 12.3(13) or

12.2XM	Tunnels	later	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; migrate to 12.3 or later	
12.2XN	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; migrate to 12.3 or later	
12.2XQ	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; migrate to 12.3 or later	
12.2XR	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(4)JA	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2XT	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; migrate to 12.3 or later	
12.2XU	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; migrate to 12.3 or later	
12.2XW	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; migrate to 12.3 or later	
	TCPv4 and Tunnels	12.2(4)YA9	

12.2YA	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; contact TAC
12.2YB	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2YC	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2YD	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2YE	TCPv4 and Tunnels	Vulnerable; migrate to 12.2S or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.2S or later
12.2YF	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2YG	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2YH	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
	TCPv4	

12.2YJ	and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2YK	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.2YL	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2YM	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2YN	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2YO	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(17d) SXB7
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.2YQ	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
	TCPv4 and	Vulnerable; migrate to 12.3(14)T

12.2YR	Tunnels	or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2YT	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Vulnerable; migrate to 12.3(12) or later
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2YU	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Vulnerable; migrate to 12.3(14)T or later
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2YV	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Vulnerable; migrate to 12.3(14)T or later
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2YW	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2YX	TCPv4 and Tunnels	Vulnerable; contact TAC
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.2YY	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3(14)T

		or later
12.2YZ	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(20)S7
	TCPv6	Vulnerable; migrate to 12.2(20)S7
	L2TPv2	Not vulnerable
12.2ZA	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(17d) SXB7
	TCPv6	Vulnerable; migrate to 12.2(17d) SXB7
	L2TPv2	Not vulnerable
12.2ZB	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2ZC	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Vulnerable; migrate to 12.3(14)T or later
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2ZD	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T
	TCPv6	Vulnerable; migrate to 12.3(14)T
	L2TPv2	Vulnerable; migrate to 12.3(14)T
12.2ZE	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Vulnerable; migrate to 12.3(12) or later
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2ZF	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Vulnerable; migrate to 12.3(14)T

		or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.2ZG	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.2ZH	TCPv4 and Tunnels	12.2(13)ZH6, available TBD	
	TCPv6	12.2(13)ZH6, available TBD	
	L2TPv2	12.2(13)ZH6, available TBD	
12.2ZJ	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.2ZK	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.2ZL	TCPv4 and Tunnels	12.2(15)ZL2, available TBD	
	TCPv6	12.2(15)ZL2, available TBD	
	L2TPv2	12.2(15)ZL2, available TBD	
	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	

12.2ZN	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.2ZP	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
Major Release		Availability of Repaired Releases	
Affected 12.3-Based Release		Rebuild	Maintenance
12.3	TCPv4 and Tunnels	12.3(3h); available 21-Apr-05	12.3(13)
		12.3(5e); available 28-Apr-05	
		12.3(6e)	
		12.3(9d); available 21-Apr-05	
		12.3(10c)	
		12.3(12b); available 12-Apr-05	
	TCPv6	12.3(6e)	12.3(12)
		12.3(3h); available 21-Apr-05	
		12.3(5e); available 28-Apr-05	
		12.3(9d); available 21-Apr-05	
12.3(10c)			
	12.3(6e)		
	12.3(3h); available 21-Apr-05		

	L2TPv2	12.3(5e); available 28- Apr-05	12.3(15), available 6-Jun- 05
		12.3(9d); available 21- Apr-05	
		12.3(12b); available 12- Apr-05	
		12.3(13a); available 2-May- 05	
12.3B	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3BC	TCPv4 and Tunnels	12.3(9a)BC2	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.3BW	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(7)T8 or later	
	TCPv6	Vulnerable; migrate to 12.3(7)T8 or later	
	L2TPv2	Vulnerable; migrate to 12.3(11)T4 or later	
12.3JA	TCPv4 and Tunnels		12.3(4)JA
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
	TCPv4 and Tunnels	12.3(7)T8	12.3(14)T
		12.3(8)T7	
		12.3(11)T4	
		12.3(7)T8	

12.3T	TCPv6	12.3(8)T7	12.3(14)T
		12.3(11)T4	
	L2TPv2	12.3(11)T4	12.3(14)T
		12.3(7)T10; available 16- May-05	
12.3XA	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3XB	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3XC	TCPv4 and Tunnels	12.3(2)XC3, available TBD	
	TCPv6	12.3(2)XC3, available TBD	
	L2TPv2	12.3(2)XC3, available TBD	
12.3XD	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3XE	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	

12.3XF	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3XG	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.3XH	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3XI	TCPv4	12.3(7)XI3	
	Tunnels	12.3(7)XI5, available TBD	
	TCPv6	12.3(7)XI3	
	L2TPv2	Vulnerable; contact TAC	
12.3XJ	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.3XK	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	

12.3XL	TCPv6	Vulnerable; migrate to 12.3(14)T or later
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.3XM	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Vulnerable; migrate to 12.3(14)T or later
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.3XQ	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Vulnerable; migrate to 12.3(14)T or later
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.3XR	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Vulnerable; migrate to 12.3(14)T or later
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.3XS	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T
	TCPv6	Vulnerable; migrate to 12.3(14)T
	L2TPv2	Vulnerable; migrate to 12.3(14)T
12.3XT	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(4)JA
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.3XU	TCPv4 and Tunnels	Vulnerable; contact TAC
	TCPv6	Vulnerable; contact TAC
	L2TPv2	Vulnerable; contact TAC

12.3XW	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(11) YF2 or later	
	TCPv6	Vulnerable; migrate to 12.3(11) YF2 or later	
	L2TPv2	Vulnerable; migrate to 12.3(11) YF2 or later	
12.3XX	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3XY	TCPv4 and Tunnels	12.3(8)XY4	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.3YA	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.3YD	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.3YF	TCPv4 and Tunnels	12.3(11)YF2, available 12-May-05	
	TCPv6	12.3(11)YF2, available 12-May-05	
	L2TPv2	12.3(11)YF2, available 12-May-05	
12.3YG	TCPv4 and Tunnels	12.3(8)YG1	

	TCPv6	12.3(8)YG1	
	L2TPv2	Vulnerable; contact TAC	
12.3YH	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.3YI	TCPv4 and Tunnels		12.3(8)YI
	TCPv6		12.3(8)YI
	L2TPv2		12.3(8)YI
12.3YJ	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.3YK	TCPv4 and Tunnels		12.3(11)YK
	TCPv6		12.3(11)YK
	L2TPv2	Vulnerable; contact TAC	
12.3YN	TCPv4 and Tunnels		12.3(11)YN
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.3YQ	TCPv4 and Tunnels		12.3(14)YQ
	TCPv6		12.3(14)YQ
	L2TPv2		12.3(14)YQ

Non-IOS-based Products

Each row of the non-IOS-based products table (below) lists the earliest possible release that contains the fix (the "First Fixed Release") and the anticipated date of availability. A product running a release that is earlier than the listed release (less than the First Fixed Release) is known to be vulnerable. The product should be upgraded at least to the indicated release or a later release (greater than or equal to the First Fixed Release label.)

Product	Bug ID	First Fixed Release
IOS XR	CSCef45332 (registered customers only)	SMU ID AA01157 for IOS XR 3.0.0. Download from https://www.cisco.com/cgi-bin/Support/FileExg/IOSXR_30.cgi SMU ID AA01172 for IOS XR 3.0.1. Download from https://www.cisco.com/cgi-bin/Support/FileExg/IOSXR_30.cgi
7960 (SCCP)	CSCef46728 (registered customers only)	7.1(1)
7970 (SCCP)	CSCef54947 (registered customers only)	6.0(3)
7960 (SIP)	CSCef54204 (registered customers only) and CSCef54206 (registered customers only)	Release date not determined yet.
Cisco PIX Security Appliance	CSCef57566 (registered customers only)	6.2.4(101) and 6.3.4(120), both available from http://www.cisco.com/pcgi-bin/tablebuild.pl/PIXPSIRT .
Catalyst 6608 and 6624	CSCsa60692 (registered customers only)	D00404000018 (load 18, DSP Ver 4.3.25) for the 6608 and A00204000010 (load 10, DSP Ver 4.3.25) for the 6624. Release date for fixed CFB and MTP loads has not been determined yet.
Cisco 11000 and 11500 Content Services Switches	CSCeh45454 (registered customers only)	Release date not determined yet.
Cisco Global Site Selector	CSCeh20083 (registered customers only)	Release date not determined yet.
Cisco MDS	CSCeh04183	

9000 Series Multilayer Switches	(registered customers only)	SAN-OS 2.1(1a)
VPN 5000 Concentrator	CSCeh59823 (registered customers only)	Please contact TAC.
ONS 15454 IOS-based blades (ML and SL)	See Cisco bug IDs for Cisco IOS	R5.0
ONS 15302 and ONS 15305	-	R2.0
Cisco MGX-8250 and MGX-8850	CSCeh65337 (registered customers only) and CSCeh63449 (registered customers only) for the Cisco MGX2	Release date not determined yet
Voice and IP Communication Products Using Cisco-Customized Microsoft Windows	-	win-OS-Upgrade-k9.2000-2-7sr3.exe; available 26-Apr-2005
Cisco ACS Solution Engine	CSCeh62307 (registered customers only)	Release date not determined yet

For all Cisco products that are based on a third party Operating System and when Cisco is not supplying the OS, please contact your respective vendor for the appropriate patches.

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

☐ Workarounds

The effectiveness of any workaround is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround is the most appropriate for use in the intended network before it is

deployed.

Effects of Disabling PMTUD

As will be shown next, one of the most common workarounds to mitigate the effect of attacks based on crafted ICMP "fragmentation needed and DF bit set" messages (or ICMPv6 "message too big" messages) is to disable PMTUD when it is possible to do so through configuration commands.

It is important to note that in general, there should not be negative side effects to disabling PMTUD. Disabling PMTUD will cause a device to send its datagrams with the DF bit cleared. When the large packets reach a small-MTU router, that router will fragment the packets into multiple smaller ones. The smaller, fragmented data will then reach the destination, where it will be reassembled into the original large packet.

Another consideration is that when PMTUD is disabled for TCP, TCP will not adjust its MSS based on changes in the Path MTU, and the actual MSS that will be used could cause unnecessary segmentation if its value is larger than the Path MTU. The MSS value that will be used will be a manually-set value (through a configuration command) or if nothing is explicitly configured, a default of 536 bytes if the destination is remote, or the outgoing interface's MTU minus 40 bytes (20 bytes for the size of the IP header and 20 bytes for the size of the TCP header) if the destination is local. To avoid unnecessary segmentation, it is recommended that the MSS be manually set to a value small enough to pass through the smallest MTU in the data path.

Note: in the particular case of Cisco IOS, the MSS value cannot be set manually (via the command **ip tcp mss <MSS value>**) when PMTUD is disabled due to an implementation detail. The actual MSS that will be used when PMTUD is disabled will be 536 bytes if the destination is remote, or the interface's MTU minus 40 bytes (1460 bytes for Ethernet, for example) if the destination is local.

Finally, please note that in general, disabling PMTUD will have no effect on existing connections, which means that existing connections must be manually terminated and re-established for the new PMTUD setting to take effect.

Voice Applications, PIX Security Appliance and PMTUD

Disabling PMTUD on devices that are running voice applications (like the Cisco CallManager) can create an undesirable condition if the voice traffic is passing through a Cisco PIX Security Appliance and the PIX Security Appliance is doing fixups of voice protocols like SCCP (**fixup protocol skinny**), SIP (**fixup protocol sip**) and H.323 (**fixup protocol h323**)


Note: the default installation of the Cisco CallManager has PMTUD disabled.

The problem occurs because the PIX Security Appliance/FWSM software cannot always fully inspect voice-signaling traffic that has segmented and/or fragmented protocol data units (PDUs). With PMTUD disabled, sufficiently large PDUs may be split across multiple TCP segments or IP fragments, which can cause a failure to properly open the pinholes for secondary connections and media traffic.

Therefore, when deciding to disable PMTUD on devices running voice applications, take care to provision the access rules to permit the necessary secondary signaling and media traffic and to disable the respective protocol's fixup.

Depending on the local security policy, the requirement of pre-opening ports may render this workaround of disabling PMTUD inapplicable.

Effects of Filtering Out ICMP Unreachable Messages

Another suggested workaround, especially in the case of IPsec and of those products where it is not possible to disable PMTUD, is to filter out ICMP "fragmentation needed and DF bit set" messages. It is important to note that any recommendation to block ICMP "fragmentation needed and DF bit set" messages applies to messages that are destined to the device that is being protected, and not for messages destined elsewhere in the network. Indiscriminately blocking ICMP unreachable messages can lead to the creation of the "black holes" described in RFC 2923 ("TCP Problems with Path MTU Discovery" - <http://www.ietf.org/rfc/rfc2923.txt> ).

Additionally, if ICMP "fragmentation needed and DF bit set" messages are blocked from being received by an end host, the end host *must* send packets with the DF bit cleared. This can be accomplished by disabling PMTUD, or, if there is no way to achieve this, by using special mechanisms like "crypto ipsec df-bit clear" where supported (in the case of IPsec).

If ICMP unreachables are being blocked, and packets are sent with the DF bit set, then the end host will never be able to react to the situation where an intermediate router needs to fragment packets that are too big for a certain PMTU; this situation requires either fragmenting the packet at the source (end host), or re-sending the packet with the DF bit cleared.

Workarounds for Cisco IOS

Transmission Control Protocol Over IP Version 4

If PMTUD has been explicitly enabled, a possible workaround to prevent PMTUD attacks is to disable it by using the global configuration command **no ip tcp path-mtu-discovery**. Once this command is executed, PMTUD will be disabled for all *new* TCP connections; configuring PMTUD on the IOS device does not have any effect on existing TCP sessions already established from/to the router.

Please note that with PMTUD disabled, the MSS that will be used will be the value set with the **ip tcp mss** command, or the default of 536 bytes for remote destinations, or 1460 bytes for local destinations.

Transmission Control Protocol Over IP Version 6

PMTUD is enabled by default when using TCP over IPv6, and it is not possible to disable it. For this reason a possible workaround is to use an ACL to block the ICMPv6 "packet too big" message.

Please note that filtering out ICMPv6 "packet too big" messages means that the layer 3 (IPv6) PMTUD is being shut down as well. Therefore, it is necessary to make sure that the MTU is set on the end host to the lowest possible IPv6 MTU - 1280 bytes. Otherwise, since the device is not seeing the "packet too big" message, the device will not know that an intermediate system has dropped a packet because it was too big.

ICMPv6 "packet too big" messages are the IPv6 equivalent to the ICMPv4 "fragmentation needed and DF bit set" message. Therefore, the same considerations presented in the section [Effects of](#)

[Filtering Out ICMP Unreachable Messages](#) apply to filtering out ICMPv6 "packet too big" messages.

IPSec

For IPSec, the recommended workaround is to "disable" PMTUD. Please note that there is not a single command to disable PMTUD under IPSec, but this can be achieved through other mechanisms. In particular, the following two things must be done:

1. Filter out ICMP "fragmentation needed and DF bit set" messages (type 3, code 4) destined to the router itself using an Access Control List or the Control Plane Policing (CoPP) feature. The following example shows how to block ICMP "fragmentation needed and DF bit set" (type 3, code 4) messages that are addressed to any of the device's IP addresses using an interface ACL (note how the type 3, code 4 message is specified using the **packet-too-big** keyword):

```
access-list 111 deny icmp any host <fa0/0's IP address> packet-too-big
access-list 111 deny icmp any host <fa0/1's IP address> packet-too-big
access-list 111 deny icmp any host <fa0/2's IP address> packet-too-big
access-list 111 permit ip any any
!
interface fastEthernet 0/0
  ip access-group 111 in
!
interface fastEthernet 0/1
  ip access-group 111 in
!
interface fastEthernet 0/2
  ip access-group 111 in
```

Note: for this workaround to be effective, all of the router's IP addresses must be included in the ACL and the ACL must be applied to all interfaces.

This type of filtering could be implemented as part of an Infrastructure ACL, which is a networking best practice. For more information on iACLs, refer to "Protecting Your Core: Infrastructure Protection Access Control Lists" at <http://www.cisco.com/warp/public/707/iacl.html>.

The following example shows how to use Control Plane Policing to accomplish the same thing:

```
access-list 140 permit icmp any host <interface0 IP address> packet-too
access-list 140 permit icmp any host <interfacel1 IP address> packet-too
[...]
access-list 140 permit icmp any host <interfaceN IP address> packet-too
access-list 140 deny ip any any
!
class-map match-all icmp-class
  match access-group 140
!
policy-map control-plane-policy
  ! Drop all traffic that matches the class "icmp-class"
  class icmp-class
    drop
!
control-plane
```

```
service-policy input control-plane-policy
```

Note: CoPP is available in IOS release trains 12.0S, 12.2S and 12.3T. Additional information on the configuration and use of the CoPP feature can be found at the following URL: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_pape

2. Allow IPsec to fragment the embedded packet even when the DF bit is set. This can be accomplished by using the command **crypto ipsec df-bit clear** (which is available in IOS 12.2 (2)T and later) or by using Policy-Based Routing (PBR) (available in IOS 12.1(6) and later) to clear the DF bit.

What follows is an example of how to use PBR to clear the DF bit:

```
route-map clear-df permit 10
  match ip address 101

!--- The following command is used to change the
!--- Don't Fragment (DF) bit value in the IP header;
!--- it must be used in route-map configuration mode.

  set ip df 0

access-list 101 permit tcp 10.1.3.0 0.0.0.255 any

interface ethernet0
  ...

!--- The following command is used to identify a
!--- route map to use for policy routing on an
!--- interface; if must be used in interface
!--- configuration mode.

ip policy route-map clear-df
```

In this example the route-map is applied to the interface where the unencrypted traffic enters the router, and 10.1.3.0/24 is the address space that is sending traffic through the IPsec tunnel.

Generic Routing Encapsulation and IPinIP

The only workaround for this case is to disable PMTUD on the tunnel interface if it has been enabled. This is accomplished via the command **no tunnel path-mtu-discovery**, while in the specific tunnel interface configuration mode.

Without the **tunnel path-mtu-discovery** command configured, the DF bit will always be cleared in the GRE IP header. This allows the GRE IP packet to be fragmented, even though the encapsulated data IP header had the DF bit set, which normally wouldn't allow the packet to be fragmented.

Please note that if you are using GRE with IPsec you need to use the command **no tunnel path-mtu-discovery** instead of the command **crypto ipsec df-bit clear** to make sure that DF bit is cleared in transmitted packets; and you also need to filter out ICMP "fragmentation needed and DF bit set" messages (type 3, code 4) destined to the router itself using an Access Control List or the Control Plane Policing (CoPP) feature as described above.

If you have an image that is fixed for Cisco Bug ID [CSCef44699](#) ([registered](#) customers only) you can set a low limit on the MTU that is learned via the PMTUD process by using the new command **tunnel path-mtu-discovery min-mtu <minimum MTU>** under the specific tunnel interface configuration mode.

Layer 2 Tunneling Protocol Version 2 and Layer 2 Tunneling Protocol Version 3

The only workaround to protect Layer 2 Tunneling Protocol sessions (both versions 2 and 3) against PMTUD attacks is to disable PMTUD if it has been enabled. For L2TPv2, this is done via the **no ip pmtu** command in **vpdn-group** configuration mode as shown here:

```
router(config)#vpdn enable
router(config)#vpdn-group 1
router(config-vpdn)#no ip pmtu
```

For L2TPv3, this is done via the commands **no ip pmtu** and **no ip dfbit set** in **pseudowire-class** configuration mode as shown here:

```
pseudowire-class [pseudowire class name]
  encapsulation l2tpv3
  no ip pmtu
  no ip dfbit set
  [...]
```

For L2TPv2, if you have an image that is fixed for Cisco Bug ID [CSCsa52807](#) ([registered](#) customers only) you can set low and high limits on the MTU that is learned via the PMTUD process by using the new commands **vpdn pmtu minimum <minimum MTU>** and **vpdn pmtu maximum <maximum MTU>** under **vpdn-group** configuration mode.

Workarounds for IOS XR

If a Cisco CRS-1 is establishing TCP sessions with other peers, then there are no configuration workarounds and customers are recommended to either apply a SMU or upgrade to a non-vulnerable version of IOS XR.

Workarounds for Cisco IP Phones

There are no workarounds for ICMP "hard" error and "source quench" attacks against Cisco IP Phones. However, these attacks can be mitigated by segmenting voice and data through the use of VLAN technologies, and in general, by following recommended best practices for IP telephony such as those documented in the white paper "SAFE: IP Telephony Security in Depth" available at http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_papers_1

Workarounds for the Cisco PIX Security Appliance

As mentioned in the [Vulnerable Products](#) section, the PIX Security Appliance is only affected if IPSec is configured and enabled. If it is affected, then there are no workarounds (since PMTUD cannot be disabled on the PIX Security Appliance) and customers are recommended to upgrade to a non-vulnerable version of the PIX Security Appliance software.

While it does not prevent PMTUD attacks, the command **clear ipsec sa** gives the administrator a

way to reset the Security Association and restore the Path MTU for the tunnel to its original value.

Workarounds for Cisco VPN 5000 Concentrator

It is possible to completely disable PMTUD by setting the configuration directive **PreTunnelFragmentation** to "no".

Even if **PreTunnelFragmentation** is left on with the "yes" setting, it is worth noting that the VPN 5000 has very strict access rules for incoming packets. If the attack were to originate from the outside (interface Ethernet 1), then the packets would always be dropped and have no effect on the IPsec connection. Packets coming across the tunnel or originating from the inside interface (Ethernet 0) would still be vulnerable to PMTUD attacks. Some customers run the device in "single-arm mode," where only Ethernet 0 is connected and terminates tunnels. Customers under this scenario are vulnerable.

Workarounds for Other Operating Systems

Cisco has products that run on top of other operating systems, like Microsoft Windows and different versions of Unix. These products normally run as end hosts, i.e. not as intermediate systems. Therefore, they may be affected by the vulnerabilities described in this document if the operating systems are vulnerable. Some of the workarounds presented in this section, in particular disabling PMTUD, may also be valid workarounds for these operating systems.

For information on how to disable Path MTU on Microsoft Windows and several versions of Unix you can consult the document "Adjusting IP MTU, TCP MSS, and PMTUD on Windows and Sun Systems" available at http://cisco.com/en/US/tech/tk870/tk877/tk880/technologies_tech_note09186a008011a218.shtml.

Protecting Against ICMP Source Quench Attacks

The ICMP "source quench" message was an early attempt at handling network congestion, but current standards recognize that it is not an effective method for handling this scenario. For this reason most modern TCP/IP implementations ignore receipt of such a message and do not send them. This situation should make it relatively safe to filter out ICMP "source quench" messages on both vulnerable devices and on the edge of your network.

Protecting Against Spoofed Packets

While considered as Network Best Practices, features like Unicast Reverse Path Forwarding (uRPF), IP source verify, DHCP Lease Query, Dynamic ACLs with AAA, and mini-ACLs (also with AAA) that help to mitigate problems that are caused by spoofed IP source addresses may be ineffective to mitigate attacks based on ICMP messages when these ICMP packets are not spoofed. The reason for this is that attackers do not necessarily need to spoof the source address of their packets to exploit this vulnerability. However, if an attacker spoofs packets, implementation of anti-spoofing mechanisms at the edge of the network will help mitigate the attack.

For more information on anti-spoofing refer to http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#sec and RFC 2827 ("Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP

Source Address Spoofing" - <http://www.ietf.org/rfc/rfc2827.txt> )

The uRPF feature of IOS helps to mitigate problems that are caused by spoofed IP source addresses. To enable uRPF, use the following commands:

```
router(config)# ip cef
router(config)# interface <interface> <interface #>

router(config-if)# ip verify unicast reverse-path
```

Please consult the feature guide [Unicast Reverse Path Forwarding Loose Mode](#) and <ftp://ftp-eng.cisco.com/cons/isp/security/URPF-ISP.pdf> for further details on how uRPF works and how to configure it in various scenarios. This is especially important if you are using asymmetric routing.

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

☐ Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

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

☐ 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>.

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

☐ Customers using Third-party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of

affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

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

☐ Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.


- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

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

☐ Exploitation and Public Announcements

The Cisco PSIRT is not aware of any malicious use of the vulnerabilities described in this advisory. NISCC is issuing a public notice of this industry-wide issue. We would like to thank Fernando Gont of Argentina's Universidad Tecnologica Nacional/Facultad Regional Haedo for reporting the ICMP "source quench" and "hard" error issues to us. Mr. Gont's full research paper on ICMP blind connection-reset and throughput-reduction attacks against TCP, including his research on the PMTU issue can be seen at <http://www.gont.com.ar/drafts/icmp-attacks-against-tcp.html> .

[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 will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- 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	2005-April-28	Added additional products that use non-Cisco-customized versions of Microsoft Windows to the list of affected products.
		<ul style="list-style-type: none">- Added the following additional products to the list of non-vulnerable products: Cisco 7902/05 and 7920 IP Phones and Cisco LocalDirector.- Added the following products to the list of vulnerable products: Cisco MGX-8250 and MGX-8850, Cisco SSL Service Module (SSLSM) (only management connections are vulnerable), and Cisco Content Switching Module (CSM) (only management connections are vulnerable).

Revision
1.2

2005-
April-
22

- Microsoft Windows is vulnerable to PMTUD attacks and attacks based on ICMP "hard" error messages according to Microsoft Security Bulletin [MS05-019](#) . All Cisco products that are shipped with, or run on top of, Microsoft Windows have been moved to the [Vulnerable Products](#) section.
- Information about the following releases in the table of fixed IOS software has been updated: 12.1(23)E4 (replaced with 12.1(23)E3), 12.1(22)E6, 12.3(11)YF2, 12.3XW, 12.3XS, 12.3XX, 12.3XR, 12.3XQ, 12.3XK, 12.3XE, 12.2EW, 12.2BZ, and 12.3XI.
- The Cisco MDS9000 is vulnerable to PMTUD attacks in addition to "source quench" attacks.
- State that for the case of GRE, IPinIP and L2TPv2 it is not possible to authenticate ICMP error messages and that the Cisco Bug IDs for these tunneling protocols add new configuration commands to set a minimum Path MTU.
- Clarify that the 6608 running Conference Bridge and Transcoder/MTP firmware are also vulnerable.
- Cisco PIX Security Appliance: 1) clarify that only traffic going through an IPSec tunnel is affected if that tunnel is attacked with a PMTUD attack, 2) clarify that version 7.0 and later of the PIX Security Appliance software is not affected by these vulnerabilities, and 3) mention the **clear ipsec sa** command as a way to restore a Path MTU in case of a PMTUD attack.
- Corrected name of first release of the Cisco-customized Microsoft Windows that has PMTUD disabled by default (2000.2.5 instead of 2000.2.6). Point out that Cisco MeetingPlace also uses this

		<p>same OS customization.</p> <ul style="list-style-type: none"> - Added link to download page for Cisco IOS XR software. - For IOS XR, emphasize that users can apply an SMU to fix the ICMP vulnerabilities instead of performing a full IOS XR upgrade. - Clarify that when PMTUD is disabled for TCP connections in Cisco IOS, the command ip tcp mss <MSS value> does not have any effect on the MSS and that the MSS that will be used will be 536 bytes or (interfaces's MTU - 40 bytes) depending on whether the destination is remote. - Clarify that when GRE is used with IPsec, the command no tunnel path-mtu-discovery should be used instead of crypto ipsec df-bit clear to clear the DF bit of transmitted packets. - GSS version 1.2 and earlier are affected. It was previously stated that it was version 1.1 and earlier.
Revision 1.1	2005-April-12	Updated Distribution section with new e-mail/Usenet news recipient: full-disclosure@lists.grok.org.uk
Revision 1.0	2005-April-12	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](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)