



Caveats for Cisco IOS Release 12.2(8)TPC10A

December 8, 2005

This document lists the resolved caveats for the Cisco 1700 series routers that support Cisco IOS Release 12.2T, up to and including Cisco IOS Release 12.2(8)TPC10A. Caveats describe unexpected behavior or defects in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

To help us improve this document, please send us your comments. If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically at <http://www.cisco.com/feedback/> or contact caveats-doc@cisco.com. For more information, see the “[Documentation Feedback](#)” section on page 16.

If You Need More Information

Cisco IOS software documentation can be found on the web through Cisco.com. For information on Cisco.com, see the “[Obtaining Documentation](#)” section on page 15.

For more information on caveats and features in Cisco IOS Release 12.2T, refer to the following sources:

- [Dictionary of Internetworking Terms and Acronyms](#)—The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this caveats document.
- [Bug Toolkit](#)—If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Service & Support: Software Center: Cisco IOS Software: BUG TOOLKIT**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)
- [Release Notes for Cisco IOS Release 12.2T](#)—These release notes describe new features and significant software components for Cisco IOS software Release 12.2T.
- [Deferral Advisories and Software Advisories for Cisco IOS Software](#)—*Deferral Advisories and Software Advisories for Cisco IOS Software* provides information about caveats that are related to deferred software images for Cisco IOS releases. If you have an account on Cisco.com, you can access *Deferral Advisories and Software Advisories for Cisco IOS Software* at <http://www.cisco.com/kobayashi/sw-center/sw-ios-advisories.shtml>.



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2005 Cisco Systems, Inc. All rights reserved.

- **What's New for IOS**—*What's New for IOS* lists recently posted Cisco IOS software releases and software releases that have been removed from Cisco.com. If you have an account on Cisco.com, you can access *What's New for IOS* at <http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml>.
- **Cisco IOS Software Roadmap**—The *Cisco IOS Software Roadmap* illustrates the relationship of the various Cisco IOS releases. If you have an account on Cisco.com, you can access the *Cisco IOS Software Roadmap* at http://www.cisco.com/warp/customer/620/roadmap_b.shtml.

**Note**

Release notes are modified only on an as-needed basis. The maintenance release number and the revision date represent the last time the release notes were modified to include new or updated information. For example, release notes are modified whenever any of the following items change: software or hardware features, feature sets, memory requirements, software deferrals for the platform, microcode or modem code, or related documents.

Hardware Supported

Cisco IOS Release 12.2(8)TPC10A supports the following Cisco 1700 series routers:

- Cisco 1701 router
- Cisco 1710 router
- Cisco 1711 router
- Cisco 1712 router
- Cisco 1720 router
- Cisco 1721 router
- Cisco 1751 and 1751-V routers
- Cisco 1760 router

Resolved Caveats—Cisco IOS Release 12.2(8)TPC10A

Cisco IOS Release 12.2(8)TPC10A is a rebuild release for Cisco IOS Release 12.2(8)T. The caveats in this section are resolved in Cisco IOS Release 12.2(8)T, but may be open in previous Cisco IOS releases.

Basic System Services

- CSCei61732
Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

Cisco has made free software available that includes the additional integrity checks for affected customers. This advisory is posted at the following URL:
<http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>.
- CSCdz32659
Symptom: Memory allocation failure (MALLOCFAIL) messages occur for a Cisco Discovery Protocol (CDP) process.

Workaround: To prevent the symptom from occurring, disable CDP by entering the **no cdp run** global configuration command.

- CSCec25430

Symptom: A Cisco device reloads on receipt of a corrupt CDP packet.

Conditions: This symptom is observed when an empty "version" field exists in the output of the **show cdp entry *** command for at least one entry.

Workaround: Disable CDP by entering the **no cdp run** global configuration command.

First alternate workaround: Disable CDP on the specific (sub-)interfaces whose corresponding neighbor(s) has or have an empty "version" field in the output of the **show cdp entry** command.

Second alternate workaround: Disconnect the 7935 or 7936 phone, in the case of the specific symptom that is described above.

- CSCed40563

Symptom: Depending upon the configuration, issuing the **show cdp entry protocol** command may cause a reload of the device.

Conditions: This symptom occurs on Cisco products that are communicating CDP with a configurable interface MTU.

Workaround: Disable CDP, making sure to issue the command under the given circumstances. You can also upgrade to a fixed version of software.

- CSCee45312

Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method to none can be bypassed.

Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.

Only the systems that are running certain versions of Cisco IOS are affected. Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

More details can be found in the security advisory which posted at the following URL:
<http://www.cisco.com/warp/public/707/cisco-sa-20050629-aaa.shtml>.

- CSCef46191

Symptoms: A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected. All other device services will operate normally.

Conditions: User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. However, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected.

Workaround: The detail advisory is available at the following URL:
<http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml>.

- CSCeg15044

Symptom: Although there are free tty lines, a Telnet connection cannot be made, and a "No Free TTYs error" message is generated.

Conditions: This symptom is observed when there are simultaneous Telnet requests.

Workaround: The **clear tcp tcb** command should clear the line.

- CSCin67568

Symptom: A Cisco device experiences a memory leak in the CDP process.

Conditions: The device sending CDP packets sends a hostname that is 256 or more characters. There are no problems with a hostname of 255 or fewer characters.

Workaround: Configure the neighbor device to use less than a 256 character hostname, or disable the CDP process with the global command **no cdp run**.

- CSCdx51428

When using AAA server for user login authentication, backup/next authentication method is used even if AAA server is available by entering a user name greater than 253 characters long.

IP Routing Protocols

- CSCdx40184

Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packeted voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml>.

- CSCdx92043

Description: If a router has IP routing disabled it will accept bogus ICMP redirect packets and modify its routing table accordingly. With IP routing disabled, the router will act as a Host, and it will comply with the Host Requirements given in the RFC1122. If IP routing is enabled (which it is by default), ICMP redirect packets are received and recognized but ignored. The router will not update its routing table with the information present in the redirect packets. By sending bogus ICMP redirect packets, a malicious user can either disrupt or intercept communication from a router. The disruption can be accomplished by advertising that a default gateway is an unused IP address from the local subnet. This will prevent the router from sending packets to any destination that is outside the local subnet.

Another possibility is to use gateway that is on the completely different subnet. If there is a device that will proxy ARP request for this bogus gateway, all victim's traffic destined outside of the local subnet may be forwarded to the bogus gateway, which would cause the victim's traffic to leak out of the local subnet to a device of attacker's choosing. If there is no device that will proxy ARP requests for a bogus gateway then the scenario collapses to the first scenario where traffic is simply blocked.

The last possibility is that malicious user inserts a default gateway whose IP address is the address of the attacker's machine itself. That way a malicious user will be able to receive all victim's traffic host that is destined outside of the local subnet. That traffic can subsequently be recorded or manipulated at the attackers' will. The traffic can even be forwarded to the correct gateway so that the victim will be unable to notice what is going on. That a malicious user could participate as a default gateway and intercept and record legitimate traffic is normal operation, and is based on availability principles, and is not dependent on the vulnerability of accepting legitimate ICMP messages.

Workaround: The router will only act upon redirects when "no ip routing" is configured. By default, a cisco router has "ip routing" enabled, and redirects are effectively ignored. If "no ip routing" is configured, this problem can still be avoided by blocking ICMP redirects with an inbound ACL.

- CSCdz41124

Symptoms: Multiple Cisco products contain vulnerabilities in the processing of Session Initiation Protocol (SIP) INVITE messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) "PROTOS" Test Suite for SIP and can be repeatedly exploited to produce a denial of service.

Conditions: This issue is observed on Cisco devices which contain support for the SIP protocol and are running vulnerable versions of software.

Workaround: Cisco will be making free software available to correct the problem as soon as possible. Additional workarounds will be documented in the Security Advisory.

This advisory is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20030221-protos.shtml>.

- CSCeb85136

Symptoms: An IP packet that is sent with an invalid IP checksum might not be dropped.

Conditions: This symptom is observed if the IP checksum is calculated with a decreased time-to-live (TTL) value. For example, in the situation where the IP checksum must be 0x1134 with a TTL of 3, if the packet is sent with an IP checksum of 0x1234 that is calculated by using a TTL value of 2, the packet is not dropped. In all other cases, packets with incorrect checksums are dropped.

Workaround: There is no workaround.

- CSCec76694

Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packeted voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml>.

- CSCee67450

A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command **bgp log-neighbor-changes** configured are vulnerable. The BGP protocol is not enabled by default, and

must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

Cisco has made free software available to address this problem.

This issue is tracked by CERT/CC VU#689326.

This advisory will be posted at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml>.

- CSCef60659

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 the following URL: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCeh13489

Symptom: A router might reset its Border Gateway Protocol (BGP) session.

Conditions: This symptom is observed when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.

Workaround: Configure the **bgp maxas limit** command so that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.

- CSCsa59600

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 the following URL:

<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 the following URL:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

TCP/IP Host-Mode Services

- CSCed27956

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>.

It describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

- CSCed38527

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>.

It describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

- CSCed78149

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 the following URL:

<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 the following URL: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

Wide-Area Networking

- CSCsa52807

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 the following URL:

<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 the following URL:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

Miscellaneous

- CSCdt13023

Symptom: A Cisco router that has run out of processor memory might unexpectedly reload due to a bus error at an invalid address, and if there is an attempt to secure shell (ssh) into a vty port, which fails due to a process creation failure. A SYS-2-CFORKMEM error message will appear immediately before the restart.

Workaround: Disable the ssh access to your router.

- CSCdv66450

Symptom: Forged IGMP packets crashes the switch when IGMP snooping is enabled.

Workaround: Disable IGMP snooping.

- CSCdw92918

Symptom: A Cisco IOS device configured for EZVPN may send packets unencrypted to the peer VPN device.

Conditions: When configured for IRB/BVI and fast-switching (CEF is disabled), an EZVPN client may send some packets in the clear (unencrypted). The packets are dropped by the peer router and connectivity is disrupted. The only packets that will be sent unencrypted are the first couple of packets of a data stream, which will not be acknowledged by the other host. TCP sessions will not be able to connect in this scenario.

Workaround: Enable CEF (Cisco Express Forwarding).

- CSCdx82139

HSRP must validate the destination IP address of packets received.

- CSCdy87221

Certain Cisco products containing support for the Secure Shell (SSH) server are vulnerable to a Denial of Service (DoS) if the SSH server is enabled on the device. A malformed SSH packet directed at the affected device can cause a reload of the device. No authentication is necessary for the packet to be received by the affected device. The SSH server in Cisco IOS is disabled by default.

Cisco will be making free software available to correct the problem as soon as possible.

The malformed packets can be generated using the SSHredder test suite from Rapid7, Inc. Workarounds are available. The Cisco PSIRT is not aware of any malicious exploitation of this vulnerability.

This advisory is available at the following URL:

<http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml>.

- CSCdz39284

Symptoms: Multiple Cisco products contain vulnerabilities in the processing of Session Initiation Protocol (SIP) INVITE messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) "PROTOS" Test Suite for SIP and can be repeatedly exploited to produce a denial of service.

Conditions: This issue is observed on Cisco devices which contain support for the SIP protocol and are running vulnerable versions of software.

Workaround: Cisco will be making free software available to correct the problem as soon as possible. Additional workarounds will be documented in the Security Advisory.

This advisory is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20030221-protos.shtml>.

- CSCdz84583

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer), and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, the attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain a TCP stack are susceptible to this vulnerability.

This advisory is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

It describes this vulnerability as it applies to Cisco products that do not run Cisco IOS software.

A companion advisory that describes this vulnerability for products that run Cisco IOS software is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>.

- CSCea19885

Symptom: A Cisco router that has a voice feature (such as H.323) enabled reloads because of a bus error at address 0xD0D0D0B.

Condition: This symptom is observed on a Cisco 3700 series, but may also occur on other routers.

Workaround: There is no workaround.

- CSCeb16876

Symptom: A Cisco router may generate a "SYS-2-GETBUF" message during the "Tag Input" process, and may subsequently reload unexpectedly.

Condition: This symptom is observed when the router fragments a Multiprotocol Label Switching (MPLS) packet.

Workaround: There is no workaround.

- CSCeb78836

Symptoms: Cisco IOS software causes a Cisco router to reload unexpectedly when the router receives a malformed H.225 setup message.

Conditions: This symptom is observed on a Cisco 1700 series that runs Cisco IOS Release 12.2(13c). The symptom occurs when the following **debug** privileged EXEC commands are enabled:

- debug h225 asn1 - debug h225 events - debug h225 q931

Workaround: There is no workaround.

- CSCeb88239

Symptom: A router that runs RIPng might crash after receiving a malformed RIPng packet, causing a Denial of Service (DoS) on the device.

Conditions: This symptom is observed when the **ipv6 debug rip** command is enabled on the router. Malformed packets can normally be sent locally. However, when the **ipv6 debug rip** command is enabled, the crash can also be triggered remotely.

Note that RIP for IPv4 is not affected by this vulnerability.

Workaround: There is no workaround.

- CSCed03333

Symptom: CBAC sessions left in sis-closing state due to out-of-order packet handling.

Workaround: None. Lowering the inspect FTP timeout will reduce exposure. Disabling CEF will reduce exposure.

Fix: Bump certain out-of-order packets to process path for catch-up and then drop packets if this is unsuccessful.

- CSCed21717

Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml>.

- CSCed35253

Symptoms: A router may reload unexpectedly after it attempts to access a low memory address.

Conditions: This symptom is observed after ACLs have been updated dynamically or after the router has responded dynamically to an IDS signature.

Workaround: Disable IP Inspect and IDS.

- CSCed65357

Symptom: The HEX representation of ALERTING TPKT is not sent in a voice call with the PI value of 8 being sent.

Workaround: There is no workaround.

- CSCed93836

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>.

This advisory describes the vulnerability as it applies to Cisco products that run Cisco IOS software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

- CSCee08584

Cisco Internetwork Operating System (IOS) Software release trains 12.1YD, 12.2T, 12.3 and 12.3T, when configured for the Cisco IOS Telephony Service (ITS), Cisco Call Manager Express (CME) or Survivable Remote Site Telephony (SRST) may contain a vulnerability in processing certain malformed control protocol messages.

A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS). This advisory is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscme.shtml>.

Cisco has made free software upgrades available to address this vulnerability for all affected customers. There are workarounds available to mitigate the effects of the vulnerability.

This vulnerability is documented by Cisco bug ID CSCee08584.

- CSCee47441

Symptom: When the Cisco IOS Firewall CBAC is configured, the router experiences a software-forced reload caused by one of the inspections processed.

Conditions: This symptom is observed when the router is part of a DMVPN hub-spoke with a Cisco VoIP phone solution deployed on it, and the router is connected to the central office over the Internet. The Cisco VoIP phone runs the SKINNY protocol.

Workaround: There is no workaround.

- CSCef44225

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 the following URL:

<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 the following URL:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCef44699

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 the following URL: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCef68324

Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

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

More details can be found in the security advisory that is posted at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>.

- CSCin56408

Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml>.

- CSCin82407

Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

This advisory will be posted at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml>.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

You can find instructions for ordering documentation at the following URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed at the following URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at the following URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at the following URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to the following URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with release notes for Cisco IOS Release 12.2T.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2005, Cisco Systems, Inc.
All rights reserved. Printed in USA.

