Cross-Platform Release Notes for Cisco IOS Release 12.3(4)TPC11

August 6, 2007

Cisco IOS Release 12.3(4)TPC11B

OL-8202-03

This document lists the resolved caveat(s) for the Cisco SOHO 90 series routers and 831 series routers that support Cisco IOS Release 12.3T, up to and including Cisco IOS Release 12.3(4)TPC11A. 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.

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, Obtaining Support, and Security Guidelines" section on page 22.

For more information on caveats and features in Cisco IOS Release 12.3T, 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 12.3T—These release notes describe new features and significant software components for Cisco IOS software Release 12.3T.

- 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.

- 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.

The most recent release notes document when this caveats document was published is *Release Notes for Cisco IOS Release 12.3T*, for Cisco IOS Release 12.3(14)T on May 2, 2005.

Hardware Supported

Cisco IOS Release 12.3(4)TPC11A supports the following Cisco routers:

- Cisco SOHO 90 series routers
    - Cisco SOHO 91 routers
    - Cisco SOHO 96 routers
    - Cisco SOHO 97 routers
- Cisco 830 series routers
    - Cisco 831 routers
    - Cisco 836 routers
    - Cisco 837 routers

Resolved Caveats—Cisco IOS Release 12.3(4)TPC11B

CSCsj66513 Traceback detected at DNQueuePeers

Symptom Traceback found at DNQueuePeers

Conditions While verifying the variable digit length dialing numbers for "Type National" and "Type International" in the numbering plan to be accepted by the network-side by using **functionality/isdn/isdn_dialPlan script**.

Workaround There is no workaround.

CSCdz55178 QoS profile name of more then 32 chars will crash the router

Symptom A router that is configured for QoS may reload unexpectedly or other serious symptoms such as memory corruption may occur.

Conditions This symptom is observed on a Cisco router that has a cable QoS profile with a name that has a length that is greater than 32 characters as in the following example:

```
cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
                          00000000011111111111222222222333^
                          123456789012345678901234567890 12|
                                                           |
                                                         PROBLEM
                                                         (Variable Overflowed).
```

Workaround Change the name of the cable QoS profile qos profile to a length that is less than 32 characters.

CSCsj66369 Traceback seen at rpmxf_dg_db_init

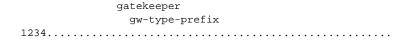**Symptom** Tracebacks seen while running metal_vpn_cases.itcl script

Conditions A strcpy in the file 'rpmxf_dg_online.c' copies more bytes than the destination buffer size. Due to this we are getting data corruption tracebacks.

Workaround There is no workaround.

CSCed26739 mm/gk/gk_cli.c:CLI:gw-type-prefix possible buffer overflow

Symptom The router will reload if "sh run" is given after a tech-prefix terminating with a large number of '.'s is configured as follows.

```
    conf t
```

REVIEW DRAFT—CISCO CONFIDENTIAL

```
         gatekeeper
           gw-type-prefix
   1234......................................................
```

Conditions

```
conf t
      gatekeeper
        gw-type-prefix
               1234......................................................
```

and enter command sh run

Workaround Do not enter long tech-prefix and using the "....." pattern

```
CSCse85200 Inadequate validation of TLVs in cdp
```

Symptom Specifically crafted CDP packets can cause a router to allocate and keep extra memory. Exploitation of this behaviour by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router.

Conditions Since CDP is a layer-2 protocol, this issue can only be triggered by systems that are residing on the same network segment.

Workaround Workaround is to disable on interfaces where CDP is not necessary.

```
CSCef61610 Incorrect handling of ICMPv6 messages can cause TCP performance
problems
```

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.

REVIEW DRAFT—CISCO CONFIDENTIAL

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.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

CSCed94829 IOS reloads due to malformed IKE messages.

Multiple Cisco products contain vulnerabilities in the processing of IPSec IKE(Internet Key Exchange) messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) "PROTOS" Test Suite for IPSec and can be repeatedly exploited to produce a denial of service.

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.This advisory is posted at: http://www.cisco.com/warp/customer/707/cisco-sa-20051114-ipsec.shtml.

CSCsb33172 short-circuit crypto engine operations when faking AM2

A vulnerability exists in the way some Cisco products handle IKE phase I messages which allows an attacker to discover which group names are configured and valid on the device. A Cisco Security Notice has been published on this issue and can be found at the following URL: http://www.cisco.com/warp/public/707/cisco-sn-20050624-vpn-grpname.shtml.

CSCek37177 Malformed tcp packets deplete processor memory.

The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition. This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.Cisco has made free software available to address this vulnerability for affected customers. This issue is documented as Cisco bug ID CSCek37177

There are workarounds available to mitigate the effects of the vulnerability.This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml.

CSCeh73049 tclsh mode bypasses aaa command authorization check.

Symptom A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (Tcl) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

Conditions Devices that are not running AAA command authorization feature, or do not support Tcl functionality are not affected by this vulnerability.This vulnerability is present in all versions of Cisco IOS that support the tclsh command.

Workaround This advisory with appropriate workarounds is posted at: http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml.

`CSCsd92405 Router crashed by repeated SSL connection with malformed finished message`

Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml

> **Note** Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
> http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

`CSCsb12598 Router forced crash on receiving fragmented TLS ClientHello`

Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml

> **Note** Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
> http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

`CSCsb40304 Router crash on sending repetitive SSL ChangeCipherSpec`

Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml

> **Note** Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
> http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

`CSCsb11124 SGBP Crafted Packet Denial of Service`

The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability. Cisco has published a Security Advisory on this issue; it is available at:
http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml

REVIEW DRAFT—CISCO CONFIDENTIAL

`CSCse05736 A router running RCP can be reloaded with a specific packet`

Symptom A router that is running RCP can be reloaded by a specific packet.

Conditions This symptom is seen under the following conditions:

- The router must have RCP enabled.
- The packet must come from the source address of the designated system configured to send RCP packets to the router.
- The packet must have a specific data content.

Workaround Put access lists on the edge of your network blocking RCP packets to prevent spoofed RSH packets. Use another protocol such as SCP. Use VTY ACLs.

`CSCsd85587 7200 Router crashes with ISAKMP Codenomicon test suite`

A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

The vulnerable cryptographic library is used in the following Cisco products:

- Cisco IOS, documented as Cisco bug ID CSCsd85587
- Cisco IOS XR, documented as Cisco bug ID CSCsg41084
- Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
- Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
- Cisco Firewall Service Module (FWSM) CSCsi97695

This vulnerability is also being tracked by CERT/CC as VU#754281.

Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

Note Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

CSCee41508 RSVP red zone crash

Symptom An IOS device may crash when processing a malformed Resource ReSerVation Protocol (RSVP) packet.

Conditions A device using an affected software version is configured for RSVP and a certain malformed RSVP packet is received.

Workaround If RSVP is required, no workaround exists. If RSVP is not required, disabling RSVP on all interfaces removes any exposure to this issue. RSVP can be disabled using the no ip rsvp bandwidth interface configuration command. The show ip rsvp EXEC command can be used on an IOS device to determine if RSVP functionality has been enabled. The show ip rsvp interface EXEC command may be used to identify the specific interfaces on which RSVP has been enabled.

CSCef48336 Corrupted OSPF Hello packets caused software forced crash

OSPF is a routing protocol defined by RFC 2328. It is designed to manage IP routing inside an Autonomous System (AS). OSPF packets use IP protocol number 89. A vulnerability exists in the processing of an OSPF packet that can be exploited to cause the reload of a system.

Since OSPF needs to process unicast packets as well as multicast packets, this vulnerability can be exploited remotely. It is also possible for an attacker to target multiple systems on the local segment at a time.

Using OSPF Authentication can be used to mitigate the effects of this vulnerability. Using OSPF Authentication is a highly recommended security best practice. A Cisco device receiving a malformed OSPF packet will reset and may take several minutes to become fully functional. This vulnerability may be exploited repeatedly resulting in an extended DOS attack.

Workaround Using OSPF Authentication OSPF authentication may be used as a workaround. OSPF packets without a valid key will not be processed. MD5 authentication is highly recommended, due to inherent weaknesses in plain text authentication. With plain text authentication, the authentication key will be sent unencrypted over the network, which can allow an attacker on a local network segment to capture the key by sniffing packets.

Refer to http://www.cisco.com/warp/public/104/25.shtml for more information about OSPF authentication. Infrastructure Access Control Lists Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The white paper "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection ACLs: http://www.cisco.com/warp/public/707/iacl.html

```
CSCsc72722 CBAC - firewall resets TCP idle timer upon receiving invalid TCP
packets.
```

Symptom TCP connections that are opened through a Cisco IOS Firewall (CBAC) may not timeout.

Conditions With Cisco IOS Firewall (CBAC) enabled, the TCP idle timer for a session may be reset even by TCP packets that fail TCP inspection and are subsequently dropped. This could lead to the TCP session not timing out.

Workaround There is no workaround

```
CSCsg16908 IOS FTP server deprecation:
```

Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information.

The IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS FTP Server service are unaffected by these vulnerabilities.

This vulnerability does not apply to the IOS FTP Client feature.

This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml

```
CSCsb93407 H323 port tcp 1720 still listening after call service stop
```

Symptom When H323 call service stops, the router still listens on TCP port 1720 and completes connection attempts.

Conditions This symptom occurs after H323 is disabled using the following configuration commands:

voice service voip

h323

call service stop

Workaround Access can be blocked by deploying an interface access list that blocks access to TCP port 1720 for traffic that is destined for any of the IP addresses of the router. For information about deploying access lists, see the "Transit Access Control Lists: Filtering at Your Edge" document at: http://www.cisco.com/warp/public/707/tacl.html

For further information about deploying access lists, see the "Protecting Your Core: Infrastructure Protection Access Control Lists" document at: http://www.cisco.com/warp/public/707/iacl.html.

For information about using control plane policing to block access to TCP port 1720, see the "Deploying Control Plane Policing White Paper" at: http://www.cisco.com/en/US/products/ps6642/products_white_paper0900aecd804fa16a.shtml.

```
CSCsf28840 Crash due to configured peer type control vector
```

A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

There are workarounds available for this vulnerability.

This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml

```
CSCsb11849 CoPP: Need support for malformed IP options
```

Symptom CoPP policy configured to drop packets with IP options will ignore packets with malformed IP options.

Conditions CoPP configured to filter ip packets with IP options.

Workaround Do not use IP option ACL filtering with CoPP. Instead configure CoPP to filter ip packets by source or destination address.

```
CSCse24889 Malformed SSH version 2 packets may cause processor memory depletion
```

Symptom Malformed SSH version 2 packets may cause a memory leak, causing the platform to operate under a degraded condition. Under rare circumstances, the platform may reload to recover itself.

Conditions This symptom is observed on a Cisco platform that is configured for SSH version 2 after it has received malformed SSHv2 packets.

Workaround As an interim solution until the affected platform can be upgraded to a Cisco IOS software image that contains the fix for caveat CSCse24889, configure SSH version 1 from the global configuration mode, as in the following example:

```
config t

ip ssh version 1 end
```

Alternate Workaround: Permit only known trusted hosts and/or networks to connect to the router by creating a vty access list, as in the following example:

```
10.1.1.0/24 is a trusted network that
is permitted access to the router, all
other access is denied

access-list 99 permit 10.1.1.0 0.0.0.255
access-list 99 deny any
line vty 0 4
access-class 99 in

end
```

Further Problem Description: For information about configuring vty access lists, see the Controlling Access to a Virtual Terminal Line document:
http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_chapter09186a0080716ec2.html

REVIEW DRAFT—CISCO CONFIDENTIAL

For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document: http://www.cisco.com/warp/public/707/ssh.shtml.

```
CSCsa54608 IOS Firewall Auth-Proxy for FTP/Telnet Sessions buffer overflow
```

The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition. Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.

Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected. Only devices running certain versions of Cisco IOS are affected. Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability. This advisory will be posted at:
http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml

```
CSCee45312 Radius authentication bypass when configured with a none fallback method
```

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

```
CSCin95836 Buffer overflow in NHRP protocol
```

Symptom A Cisco IOS device configured for NHRP may restart.

Workaround There is no workaround.

```
CSCei61732 Additional data integrity check in system timer
```

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: http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml

CSCek26492 Enhancements to Packet Input Path.

Symptom A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:
http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

Conditions This Bug resolves a symptom of CSCec71950. Cisco IOS with this specific Bug are not at risk of crash if CSCec71950 has been resolved in the software.

Workaround Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:
http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

CSCec71950 Crafted IP Option may cause DoS or code execution.

Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability. This vulnerability was discovered during internal testing. This advisory is available at:

http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

Resolved Caveats—Cisco IOS Release 12.3(4)TPC11A

Cisco IOS Release 12.3(4)TPC11A is a rebuild release for Cisco IOS Release 12.3(4)TPC11. The caveats in this section are resolved in Cisco IOS Release 12.3(4)TPC11A 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 http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml

- 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 of **none** can be bypassed.

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

  Only the systems that are running certain versions of Cisco IOS are affected. Not all configurations using RADIUS and fallback method of **none** are vulnerable to this issue. Some configurations using RADIUS, fallback method of **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 is posted at the following URL http://www.cisco.com/warp/public/707/cisco-sa-20050629-aaa.shtml.

- CSCef49904

  Symptom: Informs can't be sourced from a particular interface.

  Conditions: The user is using informs and wants them to go out on a particular interface.

  Workaround: There is no workaround.

- CSCeg15044

  Symptom: Although there are free tty lines, the user cannot make a Telnet connection and a "No Free TTYs Error" message is generated.

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

  Workaround: There is no workaround.

IP Routing Protocols

- CSCef48336

  OSPF is a routing protocol defined by RFC 2328. It is designed to manage IP routing inside an Autonomous System (AS). OSPF packets use IP protocol number 89.

  A vulnerability exists in the processing of an OSPF packet that can be exploited to cause the reload of a system.

  Since OSPF needs to process unicast packets as well as multicast packets, this vulnerability can be exploited remotely. It is also possible for an attacker to target multiple systems on the local segment at a time.

  Using OSPF Authentication can be used to mitigate the effects of this vulnerability. Using OSPF Authentication is a highly recommended security best practice

  A Cisco device receiving a malformed OSPF packet will reset and may take several minutes to become fully functional. This vulnerability may be exploited repeatedly resulting in an extended DOS attack.

  Workarounds: Using OSPF Authentication

  OSPF authentication may be used as a workaround. OSPF packets without a valid key will not be processed. MD5 authentication is highly recommended, due to inherent weaknesses in plain text authentication. With plain text authentication, the authentication key will be sent unencrypted over the network, which can allow an attacker on a local network segment to capture the key by sniffing packets.

  Refer to http://www.cisco.com/warp/public/104/25.shtml for more information about OSPF authentication.

  Infrastructure Access Control Lists

  Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The white paper "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection ACLs: http://www.cisco.com/warp/public/707/iacl.html

- CSCef61610

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

- 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.

REVIEW DRAFT—CISCO CONFIDENTIAL

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.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCef43691

  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.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- 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.

REVIEW DRAFT—CISCO CONFIDENTIAL

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.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCeh13489

  Symptom: A router may 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 in such as way 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 the event recorded 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 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.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCeg56928

  Configuring multiple static NAT translations with the extendable keyword results in only the first entry being installed in the running configuration.

  Workaround: There is no workaround.

Wide Area Networking

- CSCed32334

  Symptom: An ISDN link on a BRI interface may fial to establish itself, and a ping may fail.

  Conditions: This symptom is observed when the BRI link is connnected through an ISDN simulator.

  Workaround: There is no workaround.

- 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"

  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 que3nch" 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. Cisco has made available free software 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. It's posting can be found at: http://www.nis-cc.gov.uk/nis-cc/docs/re-20050412-00303/pdf?lang=en.

- CSCsa57082

  Symptoms: Radius Attribute 61 (NAS-PORT-TYPE) is incorrectly reported as "Virtual" to radius instead of "ASYNC" or ISND."

  Conditions: This symptom occurs when using a non-Cisco L2TP Access Concentrator (LAC) that does not support draft 1 or higher of RFC2661 in a VPDN setup with a Cisco 7200 multihop node.

  Workaround: There is no workaround.

REVIEW DRAFT—CISCO CONFIDENTIAL

Miscellaneous

- CSCsa54608

  The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition.

  Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.

  Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected.

  Only devices running certain versions of Cisco IOS are affected.

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

  This advisory will be posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml

- CSCed03333

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

  Workaround: There is no workaround. 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 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
  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCed65357

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

  Workaround: There is no workaround.

Additional References

The following sections describe the documentation available for the Cisco 1700 series routers. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com and http://www.cisco.com/univercd/home/index.htm.

Use these release notes with these documents:

- Release-Specific Documents
- Platform-Specific Documents
- Cisco IOS Software Documentation Set

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.3 and are located on Cisco.com and http://www.cisco.com/univercd/home/index.htm:

- Cross-Platform Release Notes for Cisco IOS Release 12.3(8)T

> ✎
>
> **Note**   Cross-Platform Release Notes for Cisco IOS Release 12.3 T are located on Cisco.com or on http://www.cisco.com/univercd/home/index.htm

- Product bulletins, field notices, and other release-specific documents at this URL:

  http://www.cisco.com/univercd/home/index.htm

- Caveats for Cisco IOS Release 12.3

  As a supplement to the caveats listed in these release notes, see *Caveats for Cisco IOS Release 12.3* and *Caveats for Cisco IOS Release 12.3T*, which contain caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.3 and Cisco IOS Release 12.3T.

- 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 go to: http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Platform-Specific Documents

These documents are available for the Cisco 1700 series routers:

On Cisco.com at: http://www.cisco.com/univercd/home/index.htm

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents.

Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.*Cisco IOS Software Documentation* is available in html or pdf form.

Select your release and click the command references, configuration guides, or any other Cisco IOS documentation you need.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feed-back, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.htmlCisco.com

Use this document in conjunction with the documents listed in the "Additional References" section.