



Release Notes for the Cisco 3600 Series Modular Access Routers for Cisco IOS Release 12.3(4)XD

April 12, 2005

Cisco IOS Release 12.3(4)XD4

OL-5155-01 Rev. C1

These release notes for the Cisco 3600 series routers describe the product-related enhancements provided in Cisco IOS Release 12.3(4)XD4. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.3(4)XD4, see “[Caveats](#)” section on [page 13](#). See also *Caveats for Cisco IOS Release 12.3 T*, which is updated for every maintenance release and is located on [Cisco.com](#) and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.3 T* located on [Cisco.com](#) and the Documentation CD-ROM.

Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/customer/tech_tips/index/fn.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/tech_tips/index/fn.html.

Contents

These release notes describe the following topics:

- [Inheritance Information, page 2](#)
- [Introduction, page 2](#)
- [Early Deployment Releases, page 3](#)
- [System Requirements, page 3](#)
- [New and Changed Information, page 7](#)
- [Limitations and Restrictions, page 12](#)
- [Current MIBs, page 12](#)



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

OL-5155-01 Rev. C1

Copyright © 2003 - 2004. Cisco Systems, Inc. All rights reserved.

- [Field Notices and Bulletins, page 13](#)
- [Caveats, page 13](#)

Inheritance Information

Cisco IOS Release 12.3(4)XD4, an early deployment release, is based on Cisco IOS Release 12.3(4)T, which in turn is based on Cisco IOS Release 12.3. Cisco IOS Release 12.3(4)T is the first early deployment maintenance release of Cisco IOS Release 12.3 T and is based on the mainline Cisco IOS Release 12.3. Refer to [Table 1](#) for more information.

All features in Cisco IOS Release 12.3(4)T are in Cisco IOS Release 12.3(4)XD4.

Table 1 *References for the Cross-Platform Release Notes for Cisco IOS Release 12.3 T and Cisco IOS Release 12.3(4)T*

Topic	Location
<ul style="list-style-type: none"> • Determining the Software Version • Upgrading to a New Software Release 	To view information about the topics in the left-hand column, click Cross-Platform System Requirements at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/xprn123/123reqs.htm
<ul style="list-style-type: none"> • New and Changed Information (Feature Descriptions) • MIBs • Important Notes 	To view information about the topics in the left-hand column for Cisco IOS Release 12.3 T, go to: http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/xprn123/123newf.htm Scroll down and click New Software Features in Cisco IOS Release 12.3(4)T , or MIBs , or Important Notes .
<ul style="list-style-type: none"> • Related Documentation • Obtaining Documentation • Obtaining Technical Assistance 	To view information about the topics in the left-hand column, go to: http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/xprn123/123docs.htm

Introduction

Cisco IOS Release 12.3(4)XD4 supports the Cisco 3640, Cisco 3640A, Cisco 3661, and Cisco 3662 modular access routers.

The Cisco 3600 series is a family of modular, multiservice access platforms for medium and large-sized offices and smaller Internet Service Providers. With more than 70 modular interface options, the Cisco 3600 family provides solutions for data, voice, video, hybrid dial access, virtual private networks (VPNs), and multiprotocol data routing. The high-performance, modular architecture protects customers' investment in network technology and integrates the functions of several devices into a single, manageable solution.

Cisco extended the successful Cisco 3600 series with the Cisco 3660 multiservice access platform. The Cisco 3660 provides higher densities, greater performance, and more expansion capabilities. The additional power and performance of the Cisco 3660 platform enables new applications, such as packetized voice aggregation and branch office ATM access ranging from T1/E1 IMA to OC-3. The Cisco 3660 modular access routers consist of two router models: Cisco 3661 and Cisco 3662.

For information on new features and Cisco IOS commands supported by Cisco IOS Release 12.3(4)XD4, see [New and Changed Information, page 7](#) and [Inheritance Information, page 2](#).

Early Deployment Releases

These release notes describe Cisco IOS Release 12.3(4)XD4 for the Cisco 3600 series routers. Cisco IOS Release 12.3(4)XD4 is an early deployment (ED) release based on Release 12.3(4)T, which in turn is based on Cisco IOS Release 12.3. Early deployment releases contain fixes to software caveats as well as support for new Cisco hardware and software features. Feature support is cumulative from release to release, unless otherwise noted.

[Table 2](#) lists new features supported by the Cisco 3600 series routers in Cisco IOS Release 12.3(4)XD4. See [Inheritance Information, page 2](#) for a list of the documentation specific to the Cisco 3600 series routers.

Table 2 Early Deployment Release New Features for the Cisco 3600 Series Routers

ED Release	Additional Software Features ¹ and MIBs ²	Additional Hardware	Hardware Availability
Cisco IOS Release 12.3(4)XD4	None	None	None
Cisco IOS Release 12.3(4)XD3	None	None	None
Cisco IOS Release 12.3(4)XD2	None	None	None
Cisco IOS Release 12.3(4)XD1	None	None	None
Cisco IOS Release 12.3(4)XD	Network Analysis Module Cisco NM-8AM-V2 and NM-16AM-V2 Analog Modem Network Modules with V.92 Lossless Compression R1 & ATM Cell Switching Static IP (AZR) and SSG Plug-and-Play	Network Analysis Module NM-8AM-V2, NM-16AM-V2	Now

1. Only major features are listed.

2. MIB = Management Information Base

System Requirements

This section describes the system requirements for Cisco IOS Release 12.3(4)XD4 and includes the following sections:

- [Memory Recommendations, page 4](#)
- [Supported Hardware, page 5](#)
- [Determining Your Software Release, page 5](#)
- [Upgrading to a New Software Release, page 5](#)
- [Feature Support, page 5](#)

Memory Recommendations

Table 3 lists the memory recommendations of the Cisco IOS feature sets for the Cisco 3600 series routers for Cisco IOS Release 12.3(4)XD4.

Cisco 3600 series routers are available with a 32-MB Flash memory card.

Table 3 Cisco Release 12.3(4)XD4 Memory Recommendations for the Cisco 3631, Cisco 3640/3640A, Cisco 3661, and Cisco 3662 Routers

Feature Set	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From
Cisco 3640/3640A				
IP Plus	c3640-is-mz	32 MB	96 MB	RAM
Enterprise Plus	c3640-js-mz	32 MB	128 MB	RAM
IP/FW/IDS Plus IPSEC 3DES	c3640-ik9o3s-mz	32 MB	128 MB	RAM
Enterprise/FW/IDS Plus IPSEC 3DES	c3640-jk9o3s-mz	32 MB	128 MB	RAM
Cisco 3660				
IP Plus (Standard Feature Set)	c3660-is-mz	32 MB	128 MB	RAM
Enterprise Plus (Standard Feature Set)	c3660-js-mz	64 MB	128 MB	RAM
IP/FW/IDS Plus IPSEC 3DES	c3660-ik9o3s-mz	64 MB	128 MB	RAM
Enterprise/FW/IDS Plus IPSEC 3DES	c3660-jk9o3s-mz	64 MB	128 MB	RAM

Supported Hardware

Cisco IOS Release 12.3(4)XD4 supports the following platforms:

- Cisco 3640, Cisco 3640A
- Cisco 3661, Cisco 3662

For detailed descriptions of the new hardware features, see the “New and Changed Information” section on page 7.

For a complete list of network modules and interface cards supported on Cisco 3600 series modular access routers, refer to the [Cisco 3600 Series Relevant Interfaces and Modules](#) table on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/hw/routers/ps274/products_relevant_interfaces_and_modules.html



Note The “Cisco 3600 Series Relevant Interfaces and Modules ” table referenced above is being updated to include the new products described in this release note.

For information about supported hardware for this platform and release, refer to the Hardware/Software Compatibility Matrix in the [Cisco Software Advisor](#) at the following location:

<http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hswmatrix.cgi>

Determining Your Software Release

To determine the version of Cisco IOS software running on the Cisco 3600 series routers, log in to the router and enter the **show version EXEC** command:

```
Router> show version
Cisco IOS Software, 3600 Software (C3640-SPSERVICESK9-MZ), Version 12.3(4)XD, RELEASE
SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by Cisco Systems, Inc.
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see *Cisco IOS Upgrade Ordering Instructions* located at: http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm.

Feature Support

Cisco IOS software is packaged in feature sets that consist of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. Each feature set contains a specific set of Cisco IOS features.

To improve the usability of the release notes documentation, Cisco IOS Release 12.3(4)XD release notes no longer contains the feature set tables. The feature-to-image mapping that was provided by the feature set tables is available through Cisco Feature Navigator.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>

For frequently asked questions about Cisco Feature Navigator, see the FAQs at the following URL:

<http://www.cisco.com/support/FeatureNav/FNFAQ.html>



Caution

Cisco IOS images with strong encryption (including, but not limited to 168-bit (3DES) data encryption feature sets) are subject to U.S. government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of U.S. government regulations. When applicable, the purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Determining Which Software Images (Feature Sets) Support a Specific Feature

To determine which software images (feature sets) in Cisco IOS Release 12.3(4)XD4 support a specific feature, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

-
- Step 1** From the Cisco Feature Navigator home page, click **Feature**.
 - Step 2** To find a feature, choose either **Search by full or partial feature name** or **Browse features in alphabetical order**. Either a list of features that match the search criteria or a list of features that begin with the number or letter selected from the ordered list appear.
 - Step 3** Select a feature from the left text box and click **Add**.



Note

To learn more about a feature in the list, click **Description**.

Repeat this step to add additional features. You can choose a maximum of 20 features for a single search.

- Step 4** Click **Continue**.
- Step 5** From the Major Release drop-down menu, choose 12.3T.
- Step 6** From the Release drop-down menu, choose the appropriate maintenance release.

- Step 7** From the Platform Family drop-down menu, choose the appropriate hardware platform. All software images (feature sets) that support the features that you selected appear.
-

Determining Which Features Are Supported in a Specific Software Image (Feature Set)

To determine which features are supported in a specific software image (feature set) in Cisco IOS Release 12.3(4)XD4, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

- Step 1** From the Cisco Feature Navigator home page, click **Compare/Release**.
- Step 2** In the "Find the features in a specific Cisco IOS release, using one of the following methods:" box, choose 12.3 T from the Cisco IOS Major Release drop-down menu.
- Step 3** Click **Continue**.
- Step 4** From the Release drop-down menu, choose the appropriate maintenance release.
- Step 5** From the Platform Family drop-down menu, choose the appropriate hardware platform.
- Step 6** From the Feature Set drop-down menu, choose the appropriate feature set. All features that are supported by the feature set (software image) that you selected appear.
-

New and Changed Information

The following sections list the new hardware products and software features supported by the Cisco 3600 series routers in Cisco IOS Release 12.3(4)XD.

For more information about these features, refer to the documents listed in the [“Related Documentation” section on page 2](#).

New Hardware and Software Features in Release 12.3(4)XD3 to Release 12.3(4)XD4

No new hardware products or software features are supported in Cisco IOS Release 12.3(4)XD3 to Release 12.3(4)XD4.

New Hardware and Software Features in Release 12.3(4)XD1 to Release 12.3(4)XD3

No new hardware products or software features are supported in Cisco IOS Release 12.3(4)XD1 to Release 12.3(4)XD3.

New Hardware Features in Release 12.3(4)XD

The following new hardware products are supported in Cisco IOS Release 12.3(4)XD:

- [Network Analysis Module](#)
- [NM-8AM-V2, NM-16AM-V2](#)

Network Analysis Module

Network Analysis Module for 2600XM/2691/3660/3700 platforms providing RMON2 and extended RMON capabilities. The NM-NAM leverages the functionality of the Cisco Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module in a network module form factor.

For additional information, refer to the *Network Analysis Module (NM-NAM)* feature module at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xd/nm_nam.htm

Restrictions

This feature has the following restrictions when used with Cisco IOS Release 12.3(4)XD.

- Network Analysis Module Release 3.2(1) or later is required.
- Online insertion and removal (OIR) is supported only on Cisco 3660 and Cisco 3745 platforms.

NM-8AM-V2, NM-16AM-V2

The NM-8AM-V2 and NM-16AM-V2 network modules (NMs) serve as integrated analog modem NMs for the modular access routers. These network modules terminate either eight or sixteen analog modem connections through POTS interfaces.

Hardware Specifications

Each network module consists of eight or sixteen analog modems.

Table 4 *Hardware Specifications for Analog Modems: Cisco 3600 Series and Cisco 2600XM Series Routers*

Characteristic	Description
Number of supported NMs	<ul style="list-style-type: none"> • Cisco 2610XM, 2620XM, 2650XM: 1 • Cisco 2691: 1 • Cisco 3660: Up to 6 • Cisco 3725: Up to 2 • Cisco 3745: Up to 4
Dial-related	<ul style="list-style-type: none"> • Autosensing International Pocket Exchange (IPX), TCP/IP, AppleTalk Remote Access (ARA), AppleTalk Control Protocol (ATCP) • Serial Line Internet Protocol (SLIP), Point-to-Point Protocol (PPP), Multilink PPP (MP) • Reverse Telnet support for LAN-based dial-out • Domain Name System (DNS) Domain Name Server support • MNP 2-4 for high performance under all line conditions
Carrier protocols	<ul style="list-style-type: none"> • ITU-T V.90 • V.92 Quick Connect • ITU-T V.34bis • ITU-T V.34 • ITU-T V.34+ up to 33,600 bps • ITU-T V.32bis • ITU-T V.32 • ITU-T V.32 turbo up to 19,200 bps • ITU-T V.22bis (with V.54 loop back) • ITU-T V.22 A/B • ITU-T V.23 at 75/1200 bps • ITU-T V.21 at 300 bps • BELL 103, & 212a
Error-correcting link access protocols	V.42 Link Access Procedure for Modems (LAPM), MNP 2-4

Table 4 Hardware Specifications for Analog Modems: Cisco 3600 Series and Cisco 2600XM Series Routers (continued)

Characteristic	Description
Fax protocols	<ul style="list-style-type: none"> • ITU-T V.17 • ITU-T V.29 • ITU-T V.27ter • ITU-T V.21 channel 2 • EIA 578 Class 2 Fax • Group 3 Class 1 and Class 2 Fax
Compression protocols	V.42bis (includes MNP 5)
Cables	16 RJ-11 connectors

New Software Features in Release 12.3(4)XD

The following new software features are supported by the Cisco 3600 series routers in Cisco IOS Release 12.3(4)XD:

- [Network Analysis Module](#)
- [Enhanced ITU-T G.168 Echo Cancellation](#)
- [Cisco NM-8AM-V2 and NM-16AM-V2 Analog Modem Network Modules with V.92](#)
- [Lossless Compression R1 & ATM Cell Switching](#)
- [Static IP \(AZR\) and SSG Plug-and-Play](#)

Network Analysis Module

The Network Analysis Module (NM-NAM) feature is a network module that monitors and analyzes network traffic for a system using extended Remote Monitoring (RMON) standards, RMON2, and other Management Information Bases (MIBs).

For additional information, refer to the *Network Analysis Module (NM-NAM)* feature module at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xd/nm_nam.htm

Enhanced ITU-T G.168 Echo Cancellation

The Enhanced ITU-T G.168 Echo Cancellation is extended to include platforms using the TI C5510 DSP. This Enhanced ITU-T G.168 Echo Cancellation is the only supported ECAN in Cisco IOS Release 12.3(4)XD except for NM-2V and Cisco AS5300.

Restrictions for G.168 Extended Echo Canceller

- The G.168 extended ECAN is supported in the Cisco AS5300 platform but not the default ECAN. The Cisco ECAN is the default for Cisco AS5300.
- The NM-2V does not support the extended EC on the Cisco 2600, Cisco 2600XM, Cisco 3600 series, Cisco 3700 series, or Cisco VG200.

Cisco NM-8AM-V2 and NM-16AM-V2 Analog Modem Network Modules with V.92

The Cisco NM-8AM-V2 and NM-16AM-V2 network modules (NMs) serve as integrated analog modem NMs for the modular access routers. These network modules terminate either eight or sixteen analog modem connections through POTS interfaces.

Key Features and Benefits

- 8 or 16 internal V.34/V.42bis/V.44/V.90/V.92 analog modems per network module
- Up to 56 Kbps data download and 14.4 Kbps fax communication
- V.92 Quick Connect and Modem-on-Hold features
- Centrally managed modem capabilities SNMP based tools used to manage the rest of the network (such as CiscoView and Cisco Works 2000)

Modem Management

- The Cisco 2600XM series, Cisco 3700 series, and Cisco 3600 series routers ship with general network management capabilities.



Note The analog modem network module is being submitted for approval worldwide, but due to specific in-country approval processes, approval dates vary. For the latest availability status, please check Cisco Connection Online at <http://www.cisco.com>.



Note For more information on the AT command set used by these modems, please check online at <http://www.cisco.com/>.

Platforms: 2610XM-2611XM; 2620XM-2621XM; 2650XM-2651XM; 2691; 3660; 3725; 3745

For additional information, refer to the *Cisco NM-8AM-V2 and NM-16AM-V2 Analog Modem Network Modules with V.92* feature module at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xd/gtnmam.htm>

Lossless Compression R1 & ATM Cell Switching

The Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source feature introduces a new compression technique in DSP firmware and add enhancements to Cisco IOS that include cell switching on ATM segmentation and reassembly (SAR), and the use of an external BITS clocking source. These new features enable Cisco multiservice routers to be used to transparently groom

and compress traffic in a wireless service provider network and enable a service provider to optimize the bandwidth used to backhaul the traffic from a cell site to the mobile central office for more efficient use of existing T1 and E1 lines.

For additional information, refer to the *Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source* feature module at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xd/gt_1lcc.htm

Static IP (AZR) and SSG Plug-and-Play

Access Zone Router (AZR) and Service Selection Gateway (SSG) features provide a centralized public wireless LAN (PWLAN) solution.

For additional information, refer to the *PWLAN Access Routers for the Cisco IOS Release 12.3(4)XD* feature module at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xd/pwlanar.htm>

Limitations and Restrictions

Refer to each feature for individual limitations and restrictions.

Current MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

Supported MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

Field Notices and Bulletins

- **Field Notices**—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at <http://www.cisco.com/warp/customer/770/index.shtml>. If you do not have a Cisco.com login account, you can find field notices at <http://www.cisco.com/warp/public/770/index.shtml>.
- **Product Bulletins**—If you have an account on Cisco.com, you can find product bulletins at <http://www.cisco.com/warp/customer/cc/general/bulletin/index.shtml>. If you do not have a Cisco.com login account, you can find product bulletins at <http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.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> or by logging in and selecting **Software Center: Cisco IOS Software: What's New for IOS**.

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only selected severity 3 caveats are included in the caveats document.

This section contains open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Cisco IOS Release 12.3 and Cisco IOS Release 12.3 T are also in Cisco IOS Release 12.3(4)XD4.

For information on caveats in Cisco IOS Release 12.3 and Cisco IOS Release 12.3 T, see [Caveats for Cisco IOS Release 12.3 T](#). These documents lists severity 1 and severity 2 caveats and only selected severity 3 caveats, and are located on Cisco.com and the Documentation CD-ROM.

Caveat numbers and brief descriptions for Release 12.3(4)XD4 are listed in this section.



Note

If you have an account on Cisco.com, you can use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to [Cisco.com](http://www.cisco.com) by clicking the Log In button on the right side, go to the drop down menu on the top bar of the page and select **Technical Support: Tools & Utilities: Software Bug Toolkit (under Troubleshooting Tools)**. Another option is to enter the following URL in your web browser or go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Open Caveats—Cisco IOS Release 12.3(4)XD4

- CSCee67450

A Cisco device running Cisco 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.

If a malformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the command 'show ip bgp neighbors' or running the command 'debug ip bgp <neighbor> updates' for a configured bgp neighbor.

Cisco has made free software available to address this problem.

For more details, please refer to this advisory, available at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml>

Resolved Caveats—Cisco IOS Release 12.3(4)XD4

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(4)XD4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 5 Resolved Caveats for Cisco IOS Release 12.3(4)XD4

DDTS ID Number	Description
CSCeb56909	<p>Cisco routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on MPLS disabled interfaces.</p> <p>The vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.</p> <p>More details can be found in the security advisory which is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050126-1es.shtml.</p>
CSCeb88239	<p>const2:crash RIPv6_input after sending 1 packet to FF02::9 M/cast Ad</p> <p>Symptoms: A router that runs RIPng may crash after receiving a malformed RIPng packet, causing a Denial of Service (DoS) on the device.</p> <p>Conditions: This symptom is observed when the ipv6 debug rip command is entered on the router. Malformed packets can normally be sent locally. However, when the ipv6 debug rip command is entered, the crash can also be triggered remotely.</p> <p>Note RIP for IPv4 is not affected by this vulnerability.</p> <p>Workaround: None.</p>

Table 5 Resolved Caveats for Cisco IOS Release 12.3(4)XD4 (continued)

DDTS ID Number	Description
CSCec79609	<p>MLPoA: Multilink interface comes up as Virtual-Access</p> <p>Symptoms: A Multilink PPP over ATM (MLPoA) bundle that is configured by using a multilink interface may come up as a virtual-access interface, but the multilink interface may remain inactive as an MLP bundle.</p> <p>Conditions: This symptom is observed after a bundle reset, which may be triggered by entering the clear interface user EXEC or privileged EXEC command for the multilink interface or for a virtual-access member.</p> <p>Workaround: None</p>
CSCec86420	<p>Symptoms: When you enter the undebug all privileged EXEC command on a Cisco router, all traffic that passes through an encrypted generic routing encapsulation (GRE) tunnel may stop.</p> <p>Conditions: This symptom is observed on a Ciscorouter that is configured with a GRE tunnel that is secured via IP Security (IPSec) and that is using Cisco Express Forwarding (CEF) switching.</p> <p>Workaround: Reinitialize CEF switching by entering the no ip cef global configuration command followed by the ip cef global configuration command.</p> <p>Alternate Workaround: Do not enter the undebug all privileged EXEC command. Rather, individually disable each debug command.</p>
CSCec88490	<p>Cosmetic Display CLI Related Issues</p> <p>Symptom: When doing a line-mode 2-wire ? in ATM mode on WIC-1SHDSL-V2, the help text displays incorrect mapping between the line number & the pins used.</p> <p>Explanation: When the DSL controller needs to be configured in 2-wire ATM mode, the line to be used has to be specified. In the help to choose the line, the pins used should be specified as: line-one Line one (RJ-11 pins 2&5) line-zero Line zero (RJ-11 pins 3&4)</p> <p>Instead the pins used are specified as: line-one Line one (RJ-11 pins 3&4) line-zero Line zero (RJ-11 pins 2&5)</p> <p>Conditions: WIC-1SHDSL-V2 in ATM mode.</p> <p>Workaround: None</p>

Table 5 Resolved Caveats for Cisco IOS Release 12.3(4)XD4 (continued)

DDTS ID Number	Description
CSCed21034	<p>atmVclTable maps all PVCs to all subinterfaces</p> <p>Symptoms:</p> <ul style="list-style-type: none"> -Each ATM PVC is linked to each ATM (sub)interface in the atmVclTable. -The atmVclTable is indexed by ifIndex. For a specific PVC, this should point to the ifIndex/interface on which this PVC is present. However, the atmVclTable contains one entry per ifIndex for each PVC. <p>Conditions: These symptoms are observed in a Cisco IOS image that contains the fix for CSCea63829.</p> <p>Workaround: None</p>
CSCed65285	<p>ssh leaks memory and buffers</p> <p>Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition.</p> <p>Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the “Workarounds” section of the full advisory for details.)</p> <p>This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml.</p>

Table 5 Resolved Caveats for Cisco IOS Release 12.3(4)XD4 (continued)

DDTS ID Number	Description
CSCed65778	<p>Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.</p> <p>Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the “Workarounds” section of the full advisory for details.)</p> <p>This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml</p>
CSCed40933	<p>Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.</p> <p>More details can be found in the security advisory, which is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml.</p>
CSCed78149	<p>TCP connections doing PMTU discovery vulnerable to spoofed ICMP pkts</p> <p>Symptoms: TCP connections may be vulnerable to spoofed ICMP packets. A spoofed ICMP packet may cause the TCP connection to use a very low segment size for 10 minutes at a time.</p> <p>Conditions: This symptom is observed when TCP connections are configured for PMTU discovery. Note that PMTU discovery is disabled by default on a router.</p> <p>Workaround: Disable PMTU discovery.</p>

Table 5 Resolved Caveats for Cisco IOS Release 12.3(4)XD4 (continued)

DDTS ID Number	Description
CSCee14958	<p>Clock glitch in the Spock FPGA and SCC sync/idle flags correction</p> <p>Symptoms: A SAR on a DSL WIC may cause reduced throughput, an increase in delay, or both because the bandwidth that is configured for the VC may be corrupted.</p> <p>Conditions: This symptom is observed on a Cisco 3700 series.</p> <p>Workaround: None</p>
CSCee56149	<p>DSLSAR: Incorrect sequence of TSI and tail pointer in the TX path</p> <p>Symptoms: Acknowledgements coming from a WIC may be lost, and the transmission may lock up. The missing acknowledgements may be recovered if the number of acknowledgements is more than one.</p> <p>Conditions: This symptom is observed on a Cisco 2600 series that is configured with an ADSL or G.SHDSL WIC.</p> <p>Workaround: If the transmission locks up, reset the interface. However, you can prevent the lock up from occurring by entering the tx-ring-limit ring-limit command on the PVC and by entering 24, 6, 5, or 2 for the <i>ring-limit</i> argument.</p>
CSCef44193	<p>Line-Rate on Line 0 not reported correctly</p> <p>Symptom: show controller DSL may show incorrect line-rate on line 0, with Release 12.3(4)XD1. If the line trains at a slower rate than the configured rate, under certain conditions the router will display the configured rate rather than the trained rate.</p> <p>Workaround: None. This is fixed in all subsequent releases.</p>

Table 5 Resolved Caveats for Cisco IOS Release 12.3(4)XD4 (continued)

DDTS ID Number	Description
CSCef46191	<p>Unable to telnet</p> <p>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.</p> <p>Conditions: User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected.</p> <p>Workaround: The detail advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml</p>
CSCef66120	<p>ATM MIBs not working properly for DSL WICs on c2600</p> <p>Symptom: ATM Subinterfaces are not present in IF-MIB.</p> <p>Conditions: Customer has a SHDSLv2 WIC operating in ATM mode.</p> <p>Workaround: None</p>
CSCeg00277	<p>Profile attributes are ignored when certificates are matched</p> <p>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.</p> <p>Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.</p> <p>This advisory will be posted to http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml</p>
CSCeg01135	<p>SHDSL-T1/E1 Related Commands should be Disabled for Cisco 2691 or higher</p> <p>Note T1/E1 mode for WIC-1SHDSL-V2 cards is not supported. Commands related to T1/E1 should not be used.</p>

Table 5 Resolved Caveats for Cisco IOS Release 12.3(4)XD4 (continued)

DDTS ID Number	Description
CSCin70150	<p>ATM subinterfaces are not added to ifTable in reformation images</p> <p>Symptoms: ATM-related MIBS cannot be used to monitor ATM subinterfaces.</p> <p>Conditions: This symptom is observed on a Cisco 2600 series and Cisco 3700 series when ATM subinterfaces are not added to the "ifTable" in ipbase-mz, ipvoice-mz, entbase-mz, and advsecurity9-mz images of Cisco IOS software.</p> <p>Workaround: None. Note that the symptom does not occur in entservicesk9-mz images of Cisco IOS software.</p>
CSCin82407	<p>XAUTH failure + Blank ack can allow Phase 2 negotiation</p> <p>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.</p> <p>Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.</p> <p>This advisory will be posted to http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml</p>

Caveat Advisories - Resolved Caveats

- CSCef60659: More stringent checks required for ICMP unreachable

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>.

- CSCsa59600: IPSec PMTUD not working [after 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 <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: L2TPv3 and UTI sessions doing PMTUD vulnerable to spoofed ICMP paks

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: IPsec (ESP-AH) doing PMTUD vulnerable to spoofed ICMP packets

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: GRE and IPinIP doing PMTUD vulnerable to spoofed ICMP packets

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>.

- 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>.

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>.

- CSCsa61864: Enhancements to L2TPv3 PMTUD may not work [Follow-up to 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>.

- CSCed78149: TCP connections doing PMTU discovery vulnerable to spoofed ICMP pkts
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>.

- CSCsa52807: L2TP doing PMTUD vulnerable to spoofed ICMP pkts
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>.

Open Caveats—Cisco IOS Release 12.3(4)XD3

There are no open caveats specific to Cisco IOS Release 12.3(4)XD3 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.3(4)XD3

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(4)XD3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 6 Resolved Caveats for Cisco IOS Release 12.3(4)XD3

DDTS ID Number	Description
CSCed84634	<p>Under High Link Utilization OAM may bring VC down on DSL ATM int</p> <p>Symptoms: Without the solution for this problem, some of the Operation, Administration, and Maintenance (OAM) packets may be lost over a permanent virtual circuit (PVC) configured on a digital subscriber line (DSL)(either ADSL or G.SHDSL) Interface which may result in the PVC flapping (going down and coming back up). The fix for this bug would introduce delay in sending the OAM requests/replies in the order of tens of milli seconds.</p> <p>Independent of this bug, the time required to send a OAM packet or respond to a OAM request packet from the far end depends the size of the data packets and the PVC bandwidth.</p> <p>Workaround: In order to improve OAM response times and as a potential means to prevent the PVC going down, configure a smaller TX RING on a PVC (which will reduce the head of line delay for OAM packets) and configure larger OAM timeouts using the oam retry command and/or reducing the frequency of the the OAM packets using the oam-pvc manage <loopback frequency in seconds> command under the PVC configuration.</p> <p>It is, however, important to note that for some applications, smaller TXRING values may introduce throughput loss. And the choice of TXRING value should be based on the delay requirements, if any, and the throughput.</p>
CSCee08584	<p>Cisco Internetwork Operating System (IOS) Software release trains 12.1YD, 12.2T, 12.3 and 12.3T, when configured for Cisco's IOS Telephony Service (ITS), Cisco CallManager Express (CME) or Survivable Remote Site Telephony (SRST) may contain a vulnerability in processing certain malformed control protocol messages.</p> <p>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 http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscme.shtml</p> <p>Cisco has made free software upgrades available to address this vulnerability for all affected customers.</p> <p>This vulnerability is documented by Cisco bug ID CSCee08584.</p>

Table 6 Resolved Caveats for Cisco IOS Release 12.3(4)XD3 (continued)

DDTS ID Number	Description
CSCee54372	<p>Perf. counters rollover on the DSLAM may bring the SHDSL line down</p> <p>Symptoms: The performance counter values (es, ses, crc, uas, losw) sent through the embedded operation channel (EOC) by the WIC-1SHDSL are occasionally interpreted as extremely high values by a third-party DSLAM.</p> <p>For example, even though the customer premise equipment (CPE) sends 0 as the CRC value, the DSLAM displays it as 65536. Depending upon the configuration of the DSLAM, the line may come DOWN due to perceived overflow of the counters, even though there is no real overflow.</p> <p>Workaround: There is no workaround.</p>
CSCee76166	<p>WIC-1-SHDSL-V2 may take long time to train with ECI DSLAM in 4-wire</p> <p>Symptoms: When multiple virtual circuits (VC) are configured, there is a possibility of losing bandwidth for one of the VCs. This may result in packet drops if the traffic on the VC pumped to the VC-configured bandwidth.</p> <p>Conditions: This will happens when more than 2 VC are configured with a specific bandwidth only.</p> <p>Workaround : Reordering the VC configuration may help. There is no workaround.</p>

Open Caveats—Cisco IOS Release 12.3(4)XD2

There are no open caveats specific to Cisco IOS Release 12.3(4)XD2 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.3(4)XD2

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(4)XD2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 7 Open Caveats for Cisco IOS Release 12.3(4)XD2

DDTS ID Number	Description
CSCed72331	<p>Internal serial interface messages pop up on SHDSL interface reset</p> <p>Symptom: The internal serial interface UP/DOWN message is seen on the console when [no] mode atm is configured in the WIC-1SHDSL-V2 module. This is seen only when the WAN interface card (WIC) is placed in a Cisco 2691 or Cisco 37xx motherboard. The internal serial interface message is not seen with Cisco 26xx and Fast Ethernet network module (FE NM) platforms.</p> <p>The same problem is seen with the WIC-1SHDSL module on the Cisco 2691 or Cisco 37xx platforms when the router boots up.</p> <p>Workaround: There is no workaround.</p>

Table 7 Open Caveats for Cisco IOS Release 12.3(4)XD2 (continued)

DDTS ID Number	Description
CSCed29194	<p>Message Display Issue:aal2_vc_sar_info_remove</p> <p>Symptom: A message “aal2_vc_sar_info_remove” appears while configuring the non AAL2 virtual circuit in a subinterface.</p> <p>Workaround: There is no workaround. This problem doesn't harm any functionality. For some customers, unwanted messages are not likely to be seen popping up during the permanent virtual circuit (PVC) configuration.</p>
CSCea58939	<p>Path confm fails on shut/no shut on WIC-GSHDSL with NM-HDV</p> <p>Symptom: Path confirmation failure messages are observed when VOIP calls are being setup and torn down by using Abacus tester, while the WIC-GSHDSL module (which is not in datapath) is shut; then, no-shut.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • Cisco 2600, Cisco 2691, and Cisco 3700 routers • Any existing images • VOIP calls are continually setup and torn down with the Abacus tester such that a high number of calls are made quickly. When more calls are made, this problem occurs more easily. • WIC-GSHDSL (which is not even in datapath) is shut, then enter the no shut command while these VOIP calls are being made. <p>Workaround: Do not make VOIP call while issuing a no-shut command to the WIC-GSHDSL module. Wait until the WIC-GSHDSL is up.</p> <p>Further Problem Description:</p> <ul style="list-style-type: none"> • The problem is likely to occur also on the WIC-1-ADSL and WIC-1-GSHDSL-V2 modules. • The problem is likely to be caused by xDSL WICs taking too much CPU time during the no shut command.
CSCed50752	<p>sh controller dsl is up but atm interface is down.</p> <p>Symptom: WIC-1-SHDSL-V2 DSL interface may be up but ATM is down.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • Cisco 2600, Cisco 2691, and Cisco 3700 routers • Any existing images <p>Workaround: There is no workaround. The ATM interface does not come up with the shut and no shut commands.</p> <p>Further Problem Description: This is only specific to WIC-1-SHDSL-V2 WIC.</p>
CSCed71659	<p>CoS Configuration under ATM Interface after Reload Router</p> <p>Symptom: On the WIC-1SHDSL-V2 module with certain DSL data rates (rates greater than 2304), configured class services like VBR-NRT 3200 3200 1 could be missing after the router is reloaded.</p> <p>Workaround: Enable the missing configuration again after reload.</p>

Table 7 Open Caveats for Cisco IOS Release 12.3(4)XD2 (continued)

DDTS ID Number	Description
CSCed14031	<p>EOC msg 17 not received by WIC-1SHDSL and WIC-1SHDSL-V2 from Alcatel DSLAM.</p> <p>Symptom: Embedded operations channels (EOC) message 17 is not received by WIC-1SHDSL and WIC-1SHDSL-V2 even though a certain third-party digital subscriber line access multiplier (DSLAM) sends it periodically. This is because the said DSLAM sends message 11 and message 17 with one 7E in between. The GTI_EOM interrupt is generated by the firmware on two consecutive 7Es. Hence, message 17 is not processed by the customer premise equipment (CPE) (SHDSL WIC). The problem has no impact on functionality or user interface.</p> <p>Workaround: There is no workaround.</p>
CSCed81135	<p>Trace backs appear when WIC-1-SHDSL-V2 is connected to ECI DSLAM.</p> <p>Symptom: This problem is seen with the ECI digital subscriber line access multiplier (DSLAM) when the WIC1-SHDSL-V2 module is configured in 4-wire mode. The problem is seen because of large number of embedded operations channels (EOC) messages. The problem does not impact any functionality. The problem has not been seen with other DSLAMs yet, but it could happen when there are large number of EOC messages or bad frame check sequence (FCS) EOC packets sent by the DSLAM.</p> <p>Workaround: There is no workaround.</p>
CSCed93090	<p>Line-mode CLI does not have option for auto line mode selection.</p> <p>Symptom: DSL line training stops if digital subscriber line access multiplier (DSLAM) switches from two-wire to four-wire or four-wire to 2-wire.</p> <p>Conditions: The WIC-1-SHDSL-V2 module will not train with the DSLAM unless the line-mode configuration is changed. Unless the line-mode matches with the DSLAM, the line may not train if the DSLAM switches from 2-wire mode to 4-wire mode or 4-wire mode to 2-wire mode.</p> <p>Workaround: Change the CPE line-mode configuration to DSLAM line-mode configuration.</p>

Open Caveats—Cisco IOS Release 12.3(4)XD1

There are no open caveats specific to Cisco IOS Release 12.3(4)XD1 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.3(4)XD1

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(4)XD1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 8 Open Caveats for Cisco IOS Release 12.3(4)XD1

DDTS ID Number	Description
CSCed27956	<p>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.</p> <p>All Cisco products which contain TCP stack are susceptible to this vulnerability.</p> <p>This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.</p> <p>A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.</p>
CSCed38527	<p>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.</p> <p>All Cisco products which contain TCP stack are susceptible to this vulnerability.</p> <p>This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.</p> <p>A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.</p>

Open Caveats—Cisco IOS Release 12.3(4)XD

This section documents possible unexpected behavior by Cisco IOS Release 12.3(4)XD and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 9 Open Caveats for Cisco IOS Release 12.3(4)XD

DDTS ID Number	Description
CSCea41044	<p>No downstream traffic if router reload during heavy traffic</p> <p>Symptoms: An asymmetric digital subscriber line (ADSL) or symmetric high-bit rate digital subscriber line (SHDSL) WAN interface card (WIC) may unexpectedly stop processing incoming (from CO to CPE) traffic.</p> <p>Conditions: These symptoms are observed when the following two conditions occur:</p> <p>The Cisco 2691/3725/3745 series is configured with an asymmetric digital subscriber line (ADSL) or symmetric high-bit rate digital subscriber line (SHDSL) WAN interface card (WIC) in the onboard slot (such as 0/0, 0/1, 0/2).</p> <p>The downstream (from CO to CPE) traffic rate exceeds the line rate, and this traffic is routed through the ADSL or SHDSL WIC. (The line rate is the maximum speed allowed by the digital subscriber line access multiplexer [DSLAM]).</p> <p>Further Problem Description: The show interface atm command indicates the packets input counter not incrementing but the show controller atm command indicates the Total Rx counter is incrementing.</p> <p>The show controller atm command also indicates the mpsc_rovr or mpsc_rcsc counter is non-zero.</p> <p>Workaround: Either use the DSL WIC on slots other than onboard, or ensure downstream traffic rate is below the line rate.</p>
CSCeb38709	<p>ATM AIM: unable to get free queue due to large number of connections</p> <p>ATM AIM is unable to get a free queue when a large number of ATM cell switched connections (120 to be exact) are created per ATM AIM. A message is displayed on the router as shown below:</p> <pre data-bbox="386 1276 1479 1514"> *Apr 13 19:42:48.223: EM block: 0x8 0x0 0x52 0x68 *Apr 13 19:42:48.223: Host block: 0x408 0x0 0x52 0x67 *Apr 13 19:42:48.223: SAR str_reg1 @ 0x3A800010, value 0x8, str_reg2 @ 0x3A800014, value 0x29212921 str_reg3 @ 0x3A800018, value 0x29212921, int_stat @ 0x3A900300, value 0x4 *Apr 13 19:42:48.223: Cmd_Q_idx 82, Ind_Q_idx 103 *Apr 13 19:42:48.223: Channel set to UBR *Apr 13 19:42:48.223: ATM AIM: unable to get free queue(1) buffer, msg 0x2D053100 0x0 0x0 0x0 0x36 </pre> <p>This happens only when all the connections are brought up at the same time. When 120 connections are brought up at the same time, 120 commands are sent to the maker. When the maker returns with the events or acknowledgments, the buffer allocated to queue/store these events is overrun resulting in the above message.</p> <p>Workaround: Reduce the number of connections or increase the buffer size. When the buffer size is increased, tracebacks are observed on the 3660 platform.</p>

Table 9 Open Caveats for Cisco IOS Release 12.3(4)XD (continued)

DDTS ID Number	Description
CSCeb53135	<p>NM-HDV is unable to handle more than 31 voice ports of clear-channel</p> <p>Symptom: The NM-HDV installed on a Cisco voice gateway cannot handle more than 6350 packets per second (PPS). If the packet rate goes beyond 6350 PPS, the NM-HDV randomly drops the packets.</p> <p>Conditions: Thirty-one voice channels configured with clear-channel codec work fine. As soon as the thirty-second voice channel comes up, packet drops are seen on the NM-HDV. In general, for any one or a combination of codecs configured on the NM-HDV, if the packet rate goes beyond 6350 PPS, the packets get dropped randomly.</p> <p>Workaround: Do not use more than 31 channels of clear-channel codec per NM-HDV. Do not configure any combination of codecs which will generate packets beyond the rate of 6350 PPS.</p>
CSCeb53645	<p>NM-HDV effective PPS rate reduces with number of NM-HDVs installed</p> <p>Symptom: Having packets drops with number of NM-HDVs installed in C3660.</p> <p>Conditions: If NM-HDVs installed in such as following combination:</p> <ol style="list-style-type: none"> 1. slot 1 and slot 3, 2. slot 2 and slot 4, 3. slot 5 and slot 6, <p>Will see packets drops. This is the platform PCI bus limitation since they shared the bus.</p> <p>Workaround: There is no workaround.</p>
CSCeb59417	<p>NLP disable test case failed on VIC VG-FXO/FXS</p> <p>Symptoms: Poor voice quality with noticeable residual echo with the non-linear processor (NLP) disabled.</p> <p>Workaround: Enable the NLP always to prevent poor voice quality.</p>
CSCeb60279	<p>Inconsistent NLP noise generation for NM-HDA FXO</p> <p>Symptoms: Voice activity detection (VAD) appears to be partially on for calls via Foreign Exchange Office (FXO) in high density analog (HDA) where VoIP dial peer being used is set to “no vad”.</p> <p>RTP packets are still being sent by the H.323 gateway, and are being received on the IP phone as witnessed by the RxCnt continuing to increase on the phone. However, after the person using the IP phone starts to speak they hear dead silence in their ear until the PSTN side starts to speak again (or scratch the microphone with their finger).</p> <p>Conditions: This problem occurs when high density analog network module (NM-HDA) with 4-port FXO Voice Expansion Modules on a Cisco 3640 running Cisco IOS Release 12.2(15)ZJ or Cisco IOS Release 12.2(15)ZJ1 when configuring the no vad command on VoIP dial peers.</p> <p>With Echo Cancellation disabled, the problem goes away. The problem is there with Echo Cancellation enabled regardless of the tail coverage time.</p> <p>Workaround: This issue does not occur when using Cisco IOS Release 12.2(15)T5, instead of Cisco IOS Release 12.2(15)ZJ1, however, using Cisco IOS Release 12.2(15)T5 removes the features provided by Cisco IOS Release 12.2ZJ.</p>

Table 9 Open Caveats for Cisco IOS Release 12.3(4)XD (continued)

DDTS ID Number	Description
CSCeb75205	<p>NM-x-AM-v2 fails to make outbound call after power cycle</p> <p>Symptoms: Sometimes NM-8-AM-V2 or NM-16-AM-V2 modems fail to make an outbound call after bootup.</p> <p>Workaround: Put the factory reset AT&F command in the chat script.</p>
CSCec42897	<p>E1 Controller is Down, DSL is up, Sh/no shut may recover</p> <p>Symptoms: E1 Controller is in down state, but DSL controller is in up state.</p> <p>Conditions: We observed that E1 in the down state can occur after several reloads. This problem is very difficult to reproduce.</p> <p>Workaround: Enter shut or no shut on the DSL controller.</p>
CSCec46740	<p>NM-8/16AM-V2: V.44 Compression Data Gets Stuck</p> <p>Symptoms: It has been observed that when passing large packets of data with certain patterns, that the traffic will seem to be stop. Sending a few additional bytes can cause the traffic to flow again.</p> <p>This problem happens when using V.44 compression. Using V.42bis compression does not present the problem.</p> <p>This problem was originally seen in diagnostics with 4-Kb packet sizes with incrementing data (0x00, 0x01, 0x02 ... 0xff, 0x00, 0x01, etc), and with a repeating pattern of 0xAB 0xBC (the ping data).</p> <p>Workaround: There is no workaround for this bug.</p>
CSCin56466	<p>Not able to differentiate nm-8-16am and nm-8-16am-enh via SNMP</p> <p>Symptoms: An SNMP query for the cardDescr and entPhysicalDescr attributes of NM-8-16-AM-V2 card returns the same values as for the NM-8-16-AM card. This problem will happen when an SNMP query is issued for the card.</p> <p>Workaround: There is no workaround.</p>

Resolved Caveats—Cisco IOS Release 12.3(4)XD

There are no resolved caveats specific to Cisco IOS Release 12.3(4)XD that require documentation in the release notes.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, 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 Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0402R)

Copyright © 2003-2004, Cisco Systems, Inc.
All rights reserved.