



# Release Notes for the Cisco 3200 Series Wireless and Mobile Routers for Cisco IOS Release 12.3(8)JK

---

**August 2, 2007**  
**Cisco IOS Release 12.3(8)JK1**  
**OL-10167-02 Second Release**

These release notes describe new features and significant software components for the Cisco 3200 Series 2.4-GHz wireless mobile interface card (WMIC), model C3201, which supports Cisco IOS Release 12.3(8)JK. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes. Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.3T* located on [Cisco.com](http://www.cisco.com) in pdf or html format.

For a list of the software caveats that apply to Release 12.3(8)JK, see the “[Caveats](#)” section on [page 6](#), and see the online *Caveats for Cisco IOS Release 12.3(8)T* document. The caveats document is updated for every 12.3T maintenance release and is located on [Cisco.com](http://www.cisco.com).

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](http://www.cisco.com), you can find field notices at [http://www.cisco.com/warp/customer/tech\\_tips/index/fn.html](http://www.cisco.com/warp/customer/tech_tips/index/fn.html). If you do not have a [Cisco.com](http://www.cisco.com) login account, you can find field notices at [http://www.cisco.com/warp/public/tech\\_tips/index/fn.html](http://www.cisco.com/warp/public/tech_tips/index/fn.html).

For information on Obtaining Documentation, Documentation Feedback, Cisco Product Security, Obtaining Technical Assistance, and Obtaining Additional Publications and Information, see the monthly What’s New, which also lists all new and revised Cisco technical documentation at:

<http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm>

## Contents

- [System Requirements, page 2](#)
- [New and Changed Information, page 4](#)
- [Limitations and Restrictions, page 6](#)



---

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

© 2007 Cisco Systems, Inc. All rights reserved.

- [Caveats, page 6](#)
- [Additional References, page 17](#)

## System Requirements

This section describes the system requirements for Cisco IOS Release 12.3(8)JK and includes the following sections:

- [Memory Requirements, page 2](#)
- [Hardware Supported, page 2](#)
- [Determining the Software Version, page 3](#)
- [Upgrading to a New Software Release, page 3](#)
- [Feature Set Tables, page 3](#)

## Memory Requirements

This section describes the memory requirements for the Cisco IOS feature sets that are supported by Cisco IOS Release 12.3(8)JK for the Cisco 3200 Series wireless and mobile routers.

**Table 1** *Memory Requirements for the Cisco 3200 Series Wireless and Mobile Routers*

Platform	Image Name	Feature Set	Image	Flash Memory <sup>1</sup>	Ram Memory
2.4-GHz Wireless Mobile Interface Card (WMIC)	Cisco 3201 WMIC WLAN	Wireless LAN	c3201-k9w7-tar	8 MB	32 MB

1. Recommended memory is the memory required considering future expansions.

## Hardware Supported

Cisco IOS Release 12.3(8)JK supports the 2.4-GHz Wireless Mobile Interface Card (WMIC) for the Cisco 3200 Series Mobile Access Router.

For descriptions of existing hardware features and supported modules, see the configuration guides and additional documents specific to the Cisco 3200 Series Mobile Access Router, which are available on Cisco.com at the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/access/mar\\_3200/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/mar_3200/index.htm)

This URL is subject to change without notice. If it changes, point your web browser to [Cisco.com](http://www.cisco.com), and click the following path:

**Technical Documentation > Access Servers & Routers > Mobile Access Router**

## Determining the Software Version

To determine which version of the Cisco IOS software is currently running on your Cisco 3200 Series wireless and mobile routers, log in to the router, and enter the **show version** EXEC command. The following sample output from the **show version** command indicates the version number on the second output line.

```
router# show version
Cisco Internetwork Operating System Software
IOS (tm) C3201 Software (C3201-K9W7-M), Version 12.2(15)JK2, RELEASE SOFTWARE (fc1)
Synched to technology version 12.2(15)T11
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Wed 06-Oct-04 13:30 by ealyon
Image text-base: 0x00003000, data-base: 0x005E4BE4
```

## Upgrading to a New Software Release

For general information about upgrading to a new software release, see the *Software Installation and Upgrade Procedures*, which are located on [Cisco.com](http://www.cisco.com).

## Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images, depending on the platform. Each feature set contains a specific set of Cisco IOS features. Cisco IOS Release 12.3(8)JK supports the same feature sets as Cisco IOS Releases 12.3, but Release 12.3(8)JK includes new features that are supported by the Cisco 3200 Series wireless and mobile routers.



### Caution

Cisco IOS images with strong encryption (including, but not limited to 168-bit [3DES] data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States will likely require an export license. Customer orders can be denied or subject to delay due to United States 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](mailto:export@cisco.com).

[Table 2](#) lists the features and feature sets that are supported in Cisco IOS Release 12.3(8)JK.

The table uses the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.



### Note

These feature set tables contain only a selected list of features, which are cumulative for Cisco IOS Release 12.3(8)*nn* early deployment releases only (*nn* identifies each early deployment release). The tables do not list all features in each image—additional features are listed in the [Cross-Platform Release Notes for Cisco IOS Release 12.3\(8\)T](#) and Cisco IOS Release 12.3(8)T documentation.

**Table 2** *Features Supported by the Cisco 3200 Series Wireless and Mobile Routers*

Feature	In	Image
Universal Workgroup Bridge	Yes	2.4-GHz WMIC only. See <a href="#">Table 1</a> for image
Multiple Client Profiles	Yes	2.4-GHz WMIC only. See <a href="#">Table 1</a> for image
EAP-TLS/FAST client support	Yes	2.4-GHz WMIC only. See <a href="#">Table 1</a> for image
World mode	Yes	2.4-GHz WMIC only. See <a href="#">Table 1</a> for image
AES 128-bit encryption	Yes	2.4-GHz WMIC only. See <a href="#">Table 1</a> for image
Sub 500ms fast roaming	Yes	2.4-GHz WMIC only. See <a href="#">Table 1</a> for image

## New and Changed Information

### New Hardware Features in Cisco IOS Release 12.3(8)JK

There are no new hardware features for this release.

### New Software Features in Cisco IOS Release 12.3(8)JK

The following sections describe the new software features supported by the Cisco 3200 Series wireless and mobile routers for Cisco IOS Release 12.3(8)JK.:

- [Universal Workgroup Bridge](#)
- [Multiple Client Profiles](#)
- [EAP-TLS/FAST Client Support](#)

#### Universal Workgroup Bridge

Universal workgroup bridge allows the Cisco 2.4-GHz WMIC as part of the Cisco 3200 series to connect to third party access points. You can configure the WMIC to support the following universal workgroup bridge features:

- **Interoperability**—The universal workgroup bridge can forward routing traffic using a non-cisco root device as a universal client. The universal workgroup bridge appears as a normal wireless client to the root device. As a root device, the WMIC supports Cisco Compatible Extension Clients, with all CCXv3 features and many CCXv4 features.
- **World Mode**—In standard world mode configuration, the WMIC passively scans for world mode only when the workgroup bridge boots up and performs a first scan. When the workgroup bridge receives a response from the root device for its world mode scan, it updates its frequency list and output power level according to the current country of operation. Thereafter, the workgroup bridge always performs an active scan.

To support operation in multiple countries or regulatory domains (such as a plane that needs to connect at an airport in NY and in London), the workgroup bridge must perform a passive scan. In this configuration, the client device (workgroup bridge / non-root bridge / repeater) obtains the country-specific list of frequency and output power levels through passive scan.

To support this operational change, add the **roaming** keyword to the **world-mode** command. This option instructs the workgroup bridge that it must always passively scanning.

The workgroup bridge uses the 802.11d option for world mode. The WMIC tries to receive information about the country-specific list of frequency and output power levels through the 802.11d Information Element.



**Note** With roaming added to the **world-mode** command, roaming takes a longer time; therefore, it is recommended only for situations in which it is required to assure continuous operation.

## Multiple Client Profiles

A universal workgroup bridge with multiple client profiles can automatically select a client profile, based on the available infrastructure and set of client profiles. A client profile consists of a service set identifier (SSID) and encryption settings that are bounded by a VLAN ID. To configure the SSID, you use the **ssid** command in global configuration mode. To configure encryption settings, you use the **interface dot11radio** command in global configuration mode.

Multiple client profiles are subject to the following constraints:

- To activate the feature, you must enable the universal workgroup bridge and multiple client profiles.
- All universal workgroup bridge limitations and constraints apply to multiple client profiles.
- Each SSID should have an assigned VLAN ID. The cipher suites and Wired Equivalent Privacy (WEP) for each SSID should be configured with the same assigned VLAN ID.
- The infrastructure SSID and guest mode should not be configured.
- Neither radio interface nor Ethernet interface should have the dot1q trunk configured.
- Fast roaming is not supported. Fast roaming is supported only through a single SSID across the entire roaming network.
- Support is provided for up to 16 multiple client profiles per WMIC.
- Activated profiles will use the first available SSID. Priority setting among SSIDs is not supported.

## EAP-TLS/FAST Client Support

Support is provided for EAP/TLS/FAST clients. The following notes apply:

- The 2.4 GHz WMIC (C3201-WMIC) supports storage of one digital certificate in VRAM memory.
- The EAP-TLS authentication mechanism requires that PKI infrastructure be in place with a Certificate Authority (CA) server. You can use both Microsoft and OpenSSL CA servers to provide the trustpoint.
- EAP-TLS authentication takes place between the client device (workgroup bridge, non-root bridge, or repeater) and the AAA server. Only the root device must support EAP-based authentication.
- The Cisco C3201 WMIC and the AAA server each obtains the CA certificate for its own key pairs.

## New Software Features in Release 12.3T

For information regarding the features supported in Cisco IOS Release 12.3T, see the Cross-Platform Release Notes and New Feature Documentation links at the following location on Cisco.com:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/tsd_products_support_series_home.html)

This URL is subject to change without notice. If it changes, point your web browser to [Cisco.com](http://www.cisco.com), and follow this path:

**Service & Support: Technical Documents > Cisco IOS Software: Release 12.3 > Release Notes > Cross-Platform Release Notes (Cisco IOS Release 12.3 T)**

## Limitations and Restrictions

The following sections describe limitations concerning the new hardware and software features supported by the Cisco 3200 Series WMIC for Release 12.3(8)JK.

- This release supports “world-mode” feature. To use this feature, the Work-group Bridge (WGB) or Non-root Bridge (NRB) should use Japan radio SKU when they are roaming between US and Japan. They should use EMEA radio SKU when they are roaming between US & Europe.
- When Simple Certificate Enrolment Protocol (SCEP) is selected to acquire certificate under “Enterprise Certificate Server (CA)” mode for CA server on Windows Server to work with Cisco ACS server, we recommend using “Windows Server 2003 Enterprise edition” as the Windows Operating System. This version of Windows Operating System allows the modification of CA server template. To interoperate SCEP with “Enterprise CA” server, it is required to modify “IPSEC (offline request)” template such that its “Enhanced Key Usage” Extension is same as that for “User” template. Use “certtmpl.msc” to modify the template and “certsrv.msc” to install the modified template.
- Global-mode SSID configuration is introduced for Cisco IOS Release 12.3(8)JK. Although you can still configure SSID parameters at the interface level, the interface level functionality is more limited than global-mode SSID, is chiefly intended for backwards compatibility with 12.2(15)JK, and will not be supported in future releases. Therefore, we recommend that you do not configure SSIDs at the interface level.
- In repeater mode, the Cisco 3200 Series 2.4-GHz WMIC supports only the following two topologies:
  - Root > repeater > WGB+MARC—The repeater is associated to root and accepts association from the workgroup bridge that is connected to the access and mobile router card (MARC).
  - Root > repeater > repeater > WGB— The repeater is associated to root and accepts association from another repeater that accepts association from a standalone workgroup bridge.

The WMIC in repeater mode cannot associate to the WMIC in root bridge, root ap-only, root access-point, or non-root bridge with wireless clients modes. In repeater mode, the WMIC in cannot accept association from the WMIC in non-root bridge or universal workgroup bridge modes. The WMIC does not support the ability of the access point mode to fall back to repeater mode when its FastEthernet interface goes down.

## Caveats

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, and severity 3 caveats are the least serious of these three severity levels.

Caveats in Cisco IOS Release 12.3(8)T are also in Cisco IOS Release 12.3(8)JK. For information on caveats in Cisco IOS Release 12.3T, see the *Caveats for Cisco IOS Release 12.3(8)T* document. This document lists severity 1 and 2 caveats; the documents are located on [Cisco.com](http://www.cisco.com).

**Note**

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](http://www.cisco.com) and click **Products and Services > Cisco IOS Software > Cisco IOS Software Releases 12.3 > Troubleshooting > Bug Toolkit**. Another option is to go to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](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.)

This section contains the following caveats information:

- [Open Caveats - Cisco IOS Release 12.3\(8\)JK1, page 7](#)
- [Resolved Caveats - Cisco IOS Release 12.3\(8\)JK1, page 7](#)
- [Open Caveats - Cisco IOS Release 12.3\(8\)JK, page 16](#)

## Open Caveats - Cisco IOS Release 12.3(8)JK1

There are no open caveats in this release

## Resolved Caveats - Cisco IOS Release 12.3(8)JK1

CSCsF04754

Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml>

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.

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.

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

**Symptom** System reloads unexpectedly or other serious side-effects such as memory corruption occur.

**Conditions** A cable qos profile with a length greater than 32 characters is configured on the system. For example:

```
cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
00000000011111111111222222222333^ 12345678901234567890123456789012 | | PROBLEM (Variable
Overflowed).
```

**Workaround** Change the qos profile name to a value less than 32 characters.

**Further Problem Description** The variable which holds the value for the string name only allows for 32 characters and the code did not properly truncate names longer than the associated buffer. This caused other locations in memory to be corrupted.

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>.

CSCsd19704 Arp table subject to overflow when sent from wired interface

When an Arp reply frame is received on management interface of the AP from a wired interface, the arp data is processed and the IP-MAC address mapping is placed into the arp table, regardless of whether or not the given IP address is on the local subnet.

By flooding the access point with arp replies containing random IP/MAC address pairs, all resources can be quickly consumed; an access point in this state is unable to associate any new wireless clients. Recovery from this state is only possible via power cycle.

CSCsj33246 - is missing show run after cmd for allowing expired-cer is issued

**Symptom** The **match cert <map> allow expired-cert** command does not take effect after a router reboot. Using the **match cert <map> allow expired-cert** command to ignore server cert expiration date during eap-tls auth on wmic.

**Workaround** Re-issue the same command to ignore the expiration date check for server cert.

**Further problem Description** After issuing the **match certificate <map> allow expired-certificate** command, it takes effect with no problem. However, the hyphen is missing in the **show run** command as the previous command shows up as **match certificate <map> allow expired certificate**.

Since the "-" is missing, in case the customer wants to save the config or the router reboots for whatever reason, this command will fail and the customer will need to re-issue the same manually.

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\\_chapter09186a0080716c2.html](http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_chapter09186a0080716c2.html)

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>

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>.

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>

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 behavior by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router.

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

**Workaround** The workaround is to disable on interfaces where CDP is not necessary.

CSCsb40304 Router crash on sending repetitive SSL ChangeCipherSpec

**Symptom** 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:

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>.

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>.

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.

CSCek37177 malformed tcp packets deplete processor memory.

**Symptom** 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](#)

**Workaround** 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>

CSCsg73790 IOD: WGB Handling of the 3-Addr & 4-Addr Dot11 Multicast pkts

CSCsj44081 Improvements in diagnostics and instrumentation

**Symptom** Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of internal data structures. This enhancement was introduced in select Cisco IOS Software releases published after April 5, 2007.

**Details:** With the new enhancement in place, IOS will emit a %DATACORRUPTION-1-DATAINCONSISTENCY error message whenever it detects an inconsistency in its internal data structures. This is a new error message. The following is an example.

The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp

```
May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
```

The error message is then followed by a traceback.

It is important to note that this error message does not imply that packet data is being corrupted. It does, however provide an early indicator of other conditions that can eventually lead to poor system performance or an IOS restart.

**Recommended Action** Collect “show tech-support” command output and open a service request with the Technical Assistance Center (TAC) or designated support organization. Pay particular attention to any other error messages or error symptoms that accompany the %DATACORRUPTION-1-DATAINCONSISTENCY message and note those to your support contact.

CSCsg40567 Memory leak found with malformed tls/ssl packets in http core process

**Symptom** Malformed SSL packets may cause a router to leak multiple memory blocks.

**Conditions** This symptom is observed on a Cisco router that has the ip http secure server command enabled.

**Workaround** Disable the ip http secure server command.

CSCsf07847 cdp may fail to discover neighbor information in releases wh CSCse85200

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

**Conditions** This issue occurs in IOS images that has the fix for [CSCse85200](#).

**Workaround** Disable CDP on interfaces where CDP is not required.

**Further Problem Description** Because CDP is a Layer-2 protocol, the symptom can only be triggered by routers that reside on the same network segment.

## Open Caveats - Cisco IOS Release 12.3(8)JK

CSCsd21968

**Symptom** Forcing SSH only on standard vty lines fails because telnet works.

CSCsd22247

**Symptom** TKIP replay was detected when transmitting WME packets.

CSCsd41284

**Symptom** WMIC crashes after issuing show crypto pki certificate <trustpoint>.

CSCsd17738

**Symptom** Repeater mode does not work and displays tracebacks.

CSCsd77517

**Symptom** the workgroup bridge is unable to pass traffic and displays traceback with AES and EAP FAST.

CSCsd31834

**Symptom** Memory leaks observed in multiple processes in WPAv2 feature testing.

CSCsd38601

**Symptom** Multiple memory leaks found with EAP WMIC client.

CSCsd38550

**Symptom** WMIC AP shows that the RADIUS server is alive when it cannot be pinged.

CSCsd41358

**Symptom** The following message is displayed too often: SSID CONFIG WARNING: [HOTSPOT]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.

CSCsd80777

**Symptom** Wireless and mobile router with universal workgroup bridge is unable to register with HA with Central WDS with AES.

CSCsd85255

**Symptom** Tracebacks appear when the universal workgroup bridge is configured using a multicast MAC address.

## Additional References

The following sections describe the documentation available for the Cisco 3200 Series 2.4-GHz wireless mobile interface card (WMIC), model C3201. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration 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 in pdf or html form.

Use these release notes with the documents listed in the following sections:

- [Release-Specific Documents, page 17](#)
- [Platform-Specific Documents, page 17](#)

## Release-Specific Documents

The following documents are specific to Release 12.3 and apply to Release 12.3(8)JK. They are located on [Cisco.com](#):

- [Cross-Platform Release Notes for Cisco IOS Release 12.3\(8\)T](#)
- [Field Notices: http://www.cisco.com/warp/public/tech\\_tips/index/fn.html](http://www.cisco.com/warp/public/tech_tips/index/fn.html).
- [Caveats for Cisco IOS Release 12.3](#) and [Caveats for Cisco IOS Release 12.3\(8\)T](#)

## Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 3200 Series 2.4-GHz wireless mobile interface card (WMIC), model C3201 are available on [Cisco.com](#) at the following location:

[http://www.cisco.com/en/US/products/hw/routers/tsd\\_products\\_support\\_category\\_home.html](http://www.cisco.com/en/US/products/hw/routers/tsd_products_support_category_home.html)

## Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.3 and Cisco IOS Release 12.3(8)JK, and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only.

## Cisco Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image. Cisco Feature Navigator is available 24 hours a day, 7 days a week.

To use Cisco Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Cisco Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

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

## 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.html>

---

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

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007, Cisco Systems, Inc. All rights reserved

