Release Notes for Cisco 3200 Series Routers with Cisco IOS Release 12.4(3)JL

First Released: August 22, 2008
Last Revised: March 31 , 2010
Cisco IOS Release 12.4(3)JL2
OL-17713-03 Third Release

These release notes describe new features and significant software components for the Cisco 3200 series routers that support Cisco IOS Release 12.4(3)JL. These release notes are updated as needed. Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.4T* and *About Cisco IOS Release Notes*.

For a list of the software caveats that apply to Cisco IOS Release 12.4(3)JL, see the "Caveats" section on page 7 and the online *Caveats for Cisco IOS Release 12.4T*. The caveats document is updated for every 12.4T maintenance release.

Contents

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

System Requirements

This section describes system requirements for Cisco IOS Release 12.4(3)JL and includes the following sections:

Memory Requirements

Table 1 lists memory requirements for the Cisco IOS feature sets supported by Cisco IOS Release 12.4(3)JL on Cisco 3200 series routers.

Table 1 Memory Requirements for Cisco 3200 Series Routers

Platform	Feature Set	Software Image	Flash Memory (MB)	DRAM Memory (MB)
3201-WMIC	Cisco 3201 Series WIRELESS LAN	c3201-k9w7-tar	8	32
3202-WMIC	Cisco 3202 Series WIRELESS LAN	c3202-k9w7-tar	8	32
3205-WMIC	Cisco 3205 Series WIRELESS LAN	c3205-k9w7-tar	16	64

Hardware Supported

Cisco IOS Release 12.4(3)JL supports the 2.4-GHz Wireless Mobile Interface Card (WMIC) for the Cisco 3200 series router.

For descriptions of existing hardware features and supported modules, see the configuration guides and additional documents specific to the Cisco 3200 series router, which are available at:

http://www.cisco.com/en/US/products/hw/routers/ps272/tsd_products_support_series_home.html

Determining the Software Version

To determine the version of Cisco IOS software currently running on your Cisco 3200 series router, see *About Cisco IOS Release Notes* located at:

http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html

Upgrading to a New Software Release

For general information about upgrading to a new software release, see *About Cisco IOS Release Notes* located at:

http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

Feature Set Tables

For information about Feature Set Tables, see *About Cisco IOS Release Notes* located at: http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

New and Changed Information

The following sections describe new features supported by Cisco 3200 series routers in 12.4(3)JL.

New Hardware Features in Cisco IOS Release 12.4(3)JL2

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(3)JL2

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(3)JL1

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(3)JL1

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(3)JL

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(3)JL

The new software features are:

Multiple Client Profile

The Multiple Client Profile (MCP) feature allows a Cisco 3201 Wireless Mobile Interface Card (WMIC) in a client station role (workgroup bridge, non-root, universal workgroup bridge) to maintain multiple client profiles—one profile for every configured service set identifier (SSID). Every profile contains authentication types and cipher suites for the corresponding SSID. This use of a profile-based system allows the various SSIDs to maintain prioritization. Profiles allow the configuration of authentication, encryption, and channel width per SSID.

For more information, see:

http://www.cisco.com/en/US/docs/routers/access/3200/software/wireless/MultClientProf.html

Dynamic MAC Address for Universal Workgroup Bridge

When you enable the Dynamic MAC address assignment, the universal workgroup bridge finds the MAC address of the client dynamically. If no MAC address of the client is found, the universal workgroup bridge uses the MAC address of the universal workgroup bridge BVI1 interface.

Note This feature is supported only on the Cisco 3200 Series 2.4-GHz card.

For more information, see:
http://www.cisco.com/en/US/docs/routers/access/3200/software/wireless/RolesAssociations.html#wp1024256

Any SSID

When any of the configured SSID profiles match with the AP, the workgroup bridge and universal workgroup bridge associate to the AP. When none of the configured SSID profiles match with the AP, the workgroup bridge and universal workgroup bridge fail to associate to the AP. This feature enables the workgroup bridge and universal workgroup bridge to associate to a guest-mode SSID configured on the AP. The workgroup bridge and universal workgroup bridge needs compatible authentication and encryption settings under the profile named “any.”

For more information, see:

http://www.cisco.com/en/US/docs/routers/access/3200/software/wireless/ServiceSetID.html

Management Frame Protection

Management Frame Protection (MFP) provides security for the management messages passed between access points (AP) and Client stations. MFP consists of two functional components: Infrastructure MFP and Client MFP.

Infrastructure MFP provides infrastructure support. Infrastructure MFP utilizes a message integrity check (MIC) across broadcast and directed management frames assists in detecting of rogue devices and denial of service attacks.

Client MFP provides client support. Client MFP protects authenticated clients from spoofed frames by preventing many of the common attacks against WLANs from becoming effective.

Note Management Frame Protection operation requires Wireless Domain Services (WDS). MFP is configured at the wireless LAN solution engine (WLSE), and you can manually configure MFP on an AP and WDS.

For more information, see:

http://www.cisco.com/en/US/docs/routers/access/3200/software/wireless/ManageFrameProt.html

Dynamic Channel Width

Cisco 3202 WMICs support dynamic channel width assignment for 4.9GHz. For 4.9GHz WMIC, the channel width setting is added into SSID profile to achieve dynamic channel bandwidth selection.

All the 3200 WMIC platforms for the following client modes: non-root, workgroup-bridge, and universal workgroup-bridge support dynamic channel width for 4.9GHz.

For more information, see:

http://www.cisco.com/en/US/docs/routers/access/3200/software/wireless/MultClientProf.html

Multiple Basic Service Set Identifier (MBSSID)

Cisco 3200 series WMICs now support up to 8 basic SSIDs (BSSIDs), which are similar to MAC addresses. This feature is support on all the WMICs. You use multiple BSSIDs to assign a unique Delivery Traffic Indication Message (DTIM) setting for each SSID and to broadcast more than one SSID in beacons.

For more information, see:

http://www.cisco.com/en/US/docs/routers/access/3200/software/wireless/ServiceSetID.html

Mobility Enhancements

This feature adds periodicity for roaming triggered by data rate shift and allows restriction of the number of channels that “client” mode scans.

For more information, see:

http://www.cisco.com/en/US/docs/routers/access/3200/software/wireless/WDSRoaming.html

New Software Features in Cisco IOS Release 12.4T

For information regarding the features supported in Cisco IOS Release 12.4T, see the Cross-Platform Release Notes links at: http://www.cisco.com/en/US/products/ps6441/prod_release_notes_list.html

Caveats

For general information on caveats and the bug toolkit, see *About Cisco IOS Release Notes* located at: http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

This section contains the following caveat information:

Open Caveats - 12.4(3)JL2

There are no open caveats in this release.

Resolved Caveats - 12.4(3)JL2

```
CSCsk62253 Crafted HTTPS packet will crash device.
```

Symptom Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:

- Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.
- Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.

Conditions Cisco has released free software updates that address these vulnerabilities. The advisory can be found at *Cisco Security Advisory: Cisco IOS Software WebVPN and SSLVPN Vulnerabilities*.

Workaround There is no workaround to mitigate these vulnerabilities.

CSCsk64158 Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability.

Symptom Several features within Cisco IOS Software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

Conditions Cisco has released free software updates that address this vulnerability.

Workaround Workarounds that mitigate this vulnerability are available in the workarounds section *Cisco Security Advisory: Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability*.

CSCsm97220 Input queue blocked by MIPv6 packets.

Symptom Devices that are running Cisco IOS Software and configured for Mobile IP Network Address Translation (NAT) Traversal feature or Mobile IPv6 are vulnerable to a denial of service (DoS) attack that may result in a blocked interface.

Workaround Cisco has released free softwate updates that address these vulnerabilities. The advisory can be found at *Cisco Security Advisory: Cisco IOS Software Mobile IP and Mobile IPv6 Vulnerabilities*.

CSCso47413 OSP: crash in osp_xml_message_parse when parsing OSP message.

Symptom An IOS running device router might crash when it receives a malformed OSP message.

Conditions Malformed messages need to come from the OSP server.

Workaround There is no workaround.

CSCsr68545 Error %DATACORRUPTION-1-DATAINCONSISTENCY when running ipsla with rtt.

Symptom Error message occurs:

```
000302: Jul 24 13:00:13.575 CDT: %DATACORRUPTION-1-DATAINCONSISTENCY: copy
error -Traceback= 0x410FD1A4 0x41119DB0 0x41138324 0x41DE571
```

Conditions IP SLA configured with RTT.

Workaround There is no workaround.

CSCsv30595 Device may crash upon receipt of malformed OSPF message

Symptom Device may crash upon receipt of malformed OSPF message.

Conditions A Cisco IOS device may crash upon receiving a malformed OSPF message.

Before the issue can be triggered, the Cisco IOS device must be able to establish adjacency with an OSPF peer. The issue will then occur when the processing an OSPF message sent by the peer.

Workaround There is no workaround. Using OSPF authentication can reduce/minimize the chance of hitting this issue.

CSCsw24700 SSLVPN sessions cause a memory leak in the device.

Symptom Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:

- Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.
- SSLVPN sessions cause a memory leak in the device - Cisco Bug ID CSCsw24700.

Conditions Cisco has released free software updates that address these vulnerabilities. The advisory can be found at *Cisco Security Advisory: Cisco IOS Software WebVPN and SSLVPN Vulnerabilities*.

Workaround There is no workaround to mitigate these vulnerabilities.

CSCsy15227 Cisco IOS Software Authentication Proxy Vulnerability.

Symptom Cisco IOS software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

Conditions Cisco has released an advisory that can be found at *Cisco Security Advisory: Cisco IOS Software Authentication Proxy Vulnerability*.

Workaround There is no workaround to mitigate this vulnerability.

CSCsz68294 3205 HWIC reports invalid SNR values.

Symptom The SNR values reported when issuing the command 'dot11 dot11Radio 0 linktest <some parts omitted> ' are incorrect, showing values of 163, 202, and others. The command was issued to check the link between a root and non-root bridge (both 3205wmics).

Non-Root-Bridge-09#dot11 dot11Radio 0 linktest packet-size 7500 interval 2
Start linktest to <mac address> , 100 7500 byte packets
Repeated every 2 seconds

FAIR (22 % retries)		Time	Strength(dBm)		SNR	SNR		Retries	
		msec	In	Out	In	Out		In	Out
Sent:	100, Avg	1	- 74	- 73	169	163	Tot:	24	20
Lost to Tgt:	0, Max	4	- 74	- 73	202	202	Max:	3	3
Lost to Src:	0, Min	1	- 75	- 76	0	0			

This appears to be cosmetic but we are not sure if this has any direct bearing upon the link performance at this time. The link stays up.

`CSCsz75186 TCP crash by watchdog timeout due to crafted TCP segment.`

Symptom Cisco IOS software is affected by a denial of service vulnerability that may allow a remote unauthenticated attacker to cause an affected device to reload or hang. The vulnerability may be triggered by a TCP segment containing crafted TCP options that is received during the TCP session establishment phase. In addition to specific, crafted TCP options, the device must have a special configuration to be affected by this vulnerability.

Workaround Cisco has released free software updates that address this vulnerability. The advisory can be found at *Cisco Security Advisory: Cisco IOS Software Crafted TCP Packet Denial of Service Vulnerability*.

`CSCtd78341 The unit of SNR should be db and not dbm.`

Symptom The unit of SNR should be db and not dbm.

Signal Strength	: -96 dBm	Connected for	: 716 seconds
Signal to Noise	: 114 dBm	Activity Timeout	: 15 seconds

Workaround There is no workaround.

`CSCte58425 3205 5 Ghz wmic not associating over 2 miles.`

Symptom MAR units - 3205 5Ghz wmic cards will not associate in root or non-root mode - distance is 2.24 miles between towers. Debug dot11 do0 trace clients rcv xmt beacon shows the root and non-root do not finish open authentication exchange due to timing and prior to handshake for WPA2-PSK/AES .

Conditions Root and non-root will not associate - MAR devices with wmics are mounted on towers and approximately 2.24 miles.

Workaround There is no workaround.

Open Caveats - 12.4(3)JL1

There are no open caveats in this release.

Resolved Caveats - 12.4(3)JL1

CSCsm27071

A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

- The configured feature may stop accepting new connections or sessions.
- The memory of the device may be consumed.
- The device may experience prolonged high CPU utilization.
- The device may reload. Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory. The advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml

CSCsg00102

Symptom SSLVPN service stops accepting any new SSLVPN connections.

Conditions A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.

CSCso04657

Symptom SSLVPN service stops accepting any new SSLVPN connections.

Conditions A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.

CSCsv04836

Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml.

CSCsu75750 Mobile station command **nvgen** wrong syntax.

Symptom When entering " mobile station period 720 threshold 65 " **Show run** displays the following output:

interface Dot11Radio0

[snip]

mobile station period period 720 threshold 65

The extra "period" in the mobile station config causes wmic to lose this command after reboot.

Conditions 12.4(3)JL release on 3201wmic.

Workaround Re-issue the mobile station command after each reboot.

CSCsv18333 WGB disassociates with outdoor Mesh AP intermittently.

Symptom When WGB associates with Mesh APs, WGB could intermittently disassociate from Mesh AP with video traffic.

Workaround Performing a **shut** and **no shut** of the dot11 radio interface will allow WGB to reassociate with Mesh AP.

CSCsv28916 Intermittent reachability delay for WGB client after roam.

Symptom The wired client of a WGB may intermittently lose reachability from the Distribution System side, following a WGB roam. The WGB client will resume reachability within 10 seconds after the reassociation.

Conditions WGB associating to the Cisco Unified Wireless Network.

Workaround There is none.

CSCsv50474 c3202 and c3205 WGB intermittently reload when associated to LWAPP APs.

Symptom WGB reloads intermittently when associated with LWAPP APs using WPA version 2 TKIP PSK.

Workaround Turn off MFP on either WLC/AP or WGB. Also, WPA version 2 TKIP PSK is not a commonly used encryption type. We recommend using WPA version 2 AES with 802.1X.

Open Caveats - 12.4(3)JL

There are no open caveats in this release.

Resolved Caveats - 12.4(3)JL

There are no resolved caveats in this release.

Additional References

Use this release note with the documents and websites in this release note and the documents listed in the following sections:

- Release-Specific Documents
- Platform-Specific Documents

Release-Specific Documents

The following documents are specific to Release 12.4 and apply to Release 12.4(3)JL.

- *Cross-Platform Release Notes for Cisco IOS Release 12.4T*
- *Cisco IOS Software Releases 12.4 Special and Early Deployments*
- *Caveats for Cisco IOS Release 12.4(3)T*

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 3200 series routers are available at:

http://www.cisco.com/en/US/products/hw/routers/ps272/tsd_products_support_series_home.html

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.

Notices

See the "Notices" section in *About Cisco IOS Release Notes* located at:

http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html

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