# Release Notes for the Cisco VG224 Analog Gateway for Cisco IOS Release 12.4(15)XY

**First Released: December 23, 2008**
**Last Revised: March 25, 2009**
**Cisco IOS Release 12.4(15)XY5**
**OL-18101-01 Initial Release**

These release notes for the Cisco VG224 analog gateway describe the product-related enhancements provided in Cisco IOS Release 12.4(15)XY. These release notes are updated as needed. Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.4T* *About Cisco IOS Release Notes*

For a list of the software caveats that apply to the Release 12.4(15)XY releases, 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

These release notes describe the following topics:



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

# Introduction

RJ-21 connector and two 10/100 Base T interfaces.

# System Requirements



## Memory Requirements

*Table 1 Cisco IOS Release 12.4(15)XY Memory Requirements for the Cisco VG224 Analog Gateway*

| Feature Set | Software Image | Flash Memory | DRAM Memory | Runs From |
|---|---|---|---|---|
| Cisco VG200 Series IP Subset/IPsec | vg224-i6k9s-mz | 64 | 128 | RAM |
| Cisco VG200 Series IP Subset/Voice | vg224-i6s-mz | 64 | 128 | |

## Supported Hardware

•

For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco VG200 series routers, which are at:

http://www.cisco.com/en/US/products/hw/gatecont/ps2250/tsd_products_support_series_home.html

## Determining Your Software Release

## Upgrading to a New Software Release

## Feature Set Tables

# New and Changed Information

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 

## New Hardware Features in Release 12.4(15)XY5

## New Software Features in Release 12.4(15)XY5

## New Hardware Features in Release 12.4(15)XY4

## New Software Features in Release 12.4(15)XY4

## New Hardware Features in Release 12.4(15)XY3

## New Software Features in Release 12.4(15)XY3

## New Hardware Features in Release 12.4(15)XY2

## New Software Features in Release 12.4(15)XY2

## New Hardware Features in Release 12.4(15)XY1

## New Software Features in Release 12.4(15)XY1


- Transparent Tunneling of QSIG over SIP-TDM Gateway, page 5

  SIP SRTP fallback to non-secure RTP, page 5

  Pass data in SIP REFER to triggered INVITE, control media-cut through on SIP 18x response, page 5

### Transparent Tunneling of QSIG over SIP-TDM Gateway

### SIP SRTP fallback to non-secure RTP

### Pass data in SIP REFER to triggered INVITE, control media-cut through on SIP 18x response

mechanism) before the call is connected (SIP 200 OK message is sent and accepted). Since most of the SIP IVR deployments use RFC 2833 to collect digits before a call is connected, the current default behavior (bidirectional media cut-through on 18x) is retained.

The Pass data in SIP REFER to triggered INVITE feature provides the ability to map SIP REFER message data into SIP INVITE messages. This new feature allows you to send customer-specific information to triggered SIP INVITE messages using Call-Info as the URL header of the SIP REFER-TO message. Further, this feature allows the gateway to take SIP REFER data and create a new SIP INVITE message to a new destination when a call is being placed to an Interactive Voice Response (IVR) endpoint and the IVR refers the call to an agent or to another IVR system.

## New Hardware Features in Release 12.4(15)XY

No new hardware features in this release.

## New Software Features in Release 12.4(15)XY

The following new software is supported in this release:


- AMR-NB and iLBC Codec Support for MGCP, page 6
- DSP Voice Quality Metrics, page 6
- Universal Voice Transcoding Support for IP-to-IP Gateways, page 6

### AMR-NB and iLBC Codec Support for MGCP

### DSP Voice Quality Metrics

service (QoS) objectives for your network. For more information, go to:
http://www.cisco.com/en/US/docs/ios/12_4t/12_4t15/vqmetric.html

### Universal Voice Transcoding Support for IP-to-IP Gateways

## New Features in Release 12.4T

# Limitations and Restrictions

# Caveats

## Open Caveats - Cisco IOS Release 12.4(15)XY5

## Resolved Caveats - Cisco IOS Release 12.4(15)XY5

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.

CSCsm97220

CSCsr29468

CSCso04657

**Symptom**

**Conditions**

CSCsk40676 C1812 12.4.15.T / certain pkt size block inside interface of ezvpn conn.

The inside interface of a Cisco router running EZVPN may become unresponsive when sending ICMP messages from a remote VPN client connection.

Occurs when LZS compression is used on a Windows Vista client.

**Workaround**

CSCse85652 HTTP should deny access if no enable password is configured.

CSCsg04630 7600BB: DHCP:STB crash MEM corruption at dhcpd_add_binding_to_radix_tree.

CSCsk32970 ccm switchover fails as ACL does not deny properly.

CSCsk58014 Module fails to boot up after reset.

CSCsk61991 dsl controller with auto linemode is down with peer in 4-wire linemode.

CSCsk63655 MGCP gateway returns 524 instead of 200 for a valid LCO param in CRCX.

the reason as "invalid local connection option" for a valid "L:" parameter in a CRCX message.

The symptoms can be observed on a router that is running Cisco IOS Interim Release 12.4(17.4)T1 or later, when the **<CmdBold>debug mgcp parser<noCmdBold>**

**<CmdBold>debug mgcp parser<noCmdBold>**

CSCsk70060 crafted packets to UDP port 2887 with AP HWIC may cause queue wedge.

CSCsk92135 UUT with ADSL over POTS card goes to hang state while booting IOS.

CSCsk93241 Chunk memory corruption on LFDp Input Proc.

CSCsl04399 PRI FAX calls failing for E1 controller.

**<CmdBold>fax rate disable<noCmdBold>**

CSCsl22080 12.4.15T: WebVPN stops working with TCP connection queue limit reached.

command shows <CmdBold>connection queue limit reached: port 443<noCmdBold> errors. The **<CmdBold>show tcp brief<noCmdBold>**

**<CmdBold>clear tcp tcb *<noCmdBold>**

**<CmdBold>clear tcp tcb *<noCmdBold>**

**Further Problem Description** **<CmdBold>clear ip route *<noCmdBold>**

snmpwalk on 'ipRouteTable' returns error - OID not increasing.

CSCso60174 Multiple duplicate descriptions found for mmoip aaa commands.

CSCsq15993 PBR is not supported in CEF switching path on 12.4(15)XY release

CSCsr15478 Input Queue Wedging.

CSCsu64215 ip tcp adjust-mss command results in packet loss for non-TCP traffic.

CSCso56129 %SYS-2-BADSHARE: Bad refcount in datagram_done monitoring cme/cue calls

CSCso66843 CUBE and CME do not change embedded SSRC in RTCP packets

CSCso67655 S2 CFD: Secure DSPFarm doesn't register after a reload of the router

CSCsq44013 View used twice with logging enabled

CSCsk62253

CSCsk42759

CSCsl62609

CSCso81854

CSCsk42419

CSCsk60020

CSCsk29999 AIM-IPS-K9:TCP intercept not entering aggressive mode

CSCsl61734 CUBE slow start h323 to sip transfer = dead air

CSCsl68798%SYS-2-PAK_SUBBLOCK_SETSIZE traceback at control_plane_init() at boot

```
*Mar 1 00:00:10.339:%SYS-2-PAK_SUBBLOCK_SETSIZE: 28 -Process= "Init", ipl= 3, pid= 3,
-Traceback= 0x601597F4 0x60260E80 0x602C3928 0x6014E588 0x6014E7E4 0x6028B680 0x6028B664
```

CSCsl88956 Primary nvram is not properly restored after it is corrupted

CSCsi01875 IPIP gateway rejects a second TCS

CSCse60897 call-manager-fallback does not allow more than 5 redirects

CSCsk09472 printf_ptr warnings still exist after CSCsj92597

CSCsl70220 Entity hierarchy issue in 1805 device

CSCsl72097 Alignment Error seen in 3800 while making E1/r2 call.

CSCsm34933 Refresh Re-Invite disconnect call because CUBE does not send out 200 OK

CSCsm44512 Router crash when unconfigure PVC from ATM interface

CSCsm44792 input gain auto-control -9 is added automatically to voice-ports.

trunk 19990929090 description #0/2/0:0#0# INUSE 1221.

CSCsl22920 - IOS gw not tunneling ISDN ALERTING message over SIP

ISDN QSIG ALERTING message received from Destination PINX is not transparently transported to Originating PINX.

This is seen if the Destination PINX sends ISDN QSIG CALL_PROC with PI==1 in response to ISDN QSIG SETUP message.

There is no workaround.

: ISDN QSIG CALL_PROC with PI==1 received from destination PINX is converted to SIP 183 Progress at TGW and hence treated as ISDN QSIG PROGRESS at OGW/Originating PINX. Due to this 183 corresponding to ISDN QSIG ALERTING from Dest PINX is dropped at OGW.

There are no resolved caveats in this release.

There are no open caveats in this release.

A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

Cisco has released free software updates that address this vulnerability.

Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-ssl.shtml.

CME with UCCX integration could crash at the following function:

```
cmm_crs_proc_tr_call_trans_req()
```

```
CSCsi69819 Line protocol down when no auto speed and duplex negotiate on onboard
FE.
```

# Additional References

- 
-

The following documents are specific to Release 12.4 and apply to Release 12.4(15)XY.

*Cisco IOS Software Releases 12.4 Special and Early Deployments*

*Caveats for Cisco IOS Release 12.4(20)T*

## Platform-Specific Documents

## Cisco IOS Software Documentation Set

### Documentation Modules

*Cisco IOS Software Documentation*

# Notices

*About Cisco IOS Release Notes*

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