Release Notes for Cisco IAD2430 Series Integrated Access Devices with Cisco IOS Release 12.4(11)XW

First Released: May 4, 2007
Last Revised: February 5, 2009
Cisco IOS Release 12.4(11)XW10
OL-13462-09 Ninth Release

These release notes for the Cisco IAD2430 Series Integrated Access Devices (IAD) describe the product-related enhancements provided in Cisco IOS Release 12.4(11)XW. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.4(11)XW, see the "Caveats" section on page 9 and the online *Caveats for Cisco IOS Release 12.4T*

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

Contents

These release notes describe the following topics:

Introduction

The Cisco IAD2430 is the next generation integrated voice and data services platform for Service Providers, building on the industry leading Cisco IAD2420 series IAD. The Cisco IAD2430 series offers a major leap forward in price performance and enhanced software functionality such as MGCP SRST used to accelerate the migration from time division multiplexing (TDM) to VoIP cost efficiently. The Cisco IAD2430 series harnesses the maturity of the Cisco IAD2420 series software and enhances functionality by providing more capabilities such as denser interfaces (up to 24 FXS and up to 2 voice or 2 data T1s), encryption, and DC power back up while maintaining it's 1RU form factor for space saving Service Provider Managed Services deployment.

For information on new features and Cisco IOS commands supported by Cisco IOS Release 12.4(11)XW, see the "New and Changed Information" section on page 6.

Cisco 2430 Series Integrated Access Device

-
- Cisco 2431-8FXS IAD
- Cisco 2431-16FXS IAD
- Cisco 2431-1T1E1 IAD

  Cisco 2432-24FXS IAD

The following WAN interface cards (WICs) and Voice Interface Cards (VICs) are supported:

VIC2-2FXO

VIC2-2FXS

VIC-4FXS/DID

VIC2-2BRI-NT/TE

VWIC-2MFT-T1

VWIC-2MFT-E1

WIC-1T

WIC-1ADSL

WIC-1SHDSL

WIC-1ADSL-DG

WIC-1SHDSL-V2

Port Numbering

-
-
-
-
- FXS voice port numbering begins at 2/0 and extends to 2/7, 2/15, or 2/23, depending on the number of voice ports.

MGCP Endpoint Naming Convention

Cisco IAD2431-1T1E1

S1/DS1-0/1@iad2430-digital
S1/DS1-0/2@iad2430-digital
. . .
S1/DS1-0/24@iad2430-digital

S1/DS1-1/1@iad2430-digital
S1/DS1-1/2@iad2430-digital
. . .
S1/DS1-1/24@iad2430-digital

Cisco IAD2430-24FXS, IAD2431-8FXS, IAD2431-16FXS, IAD2432-24FXS

Voice Analog Ports

System Requirements

-
-
-
-
-

Memory Requirements

Table 1 Cisco Release 12.4(11)XW Memory Recommendations for the Cisco IAD2430 Series IAD

Platform	Feature Set	Software Image	Recommended Flash Memory (MB)	Recommended DRAM Memory (MB)	Runs From
		c2430-i6k9o3s-mz	64	128	RAM
	Cisco 2430 Series IOS IP Subset/Voice	c2430-i6s-mz	64	128	RAM
Cisco IAD2431-Cisco IAD2432	Cisco 2430 Series IOS IP Plus/IPsec 64BIT/FW/Voice	c2430-ik9o3s-mz	64	128	RAM
	Cisco 2430 Series IOS IP Plus	c2430-is-mz	64	128	RAM

Hardware Supported

-
-
-

http://www.cisco.com/en/US/products/hw/gatecont/ps887/tsd_products_support_series_home.html

Determining the Software Version

About Cisco IOS Release Notes

Upgrading to a New Software Release

Feature Set Tables

New and Changed Information

New Hardware Features in Cisco IOS Release 12.4(11)XW10

New Software Features in Cisco IOS Release 12.4(11)XW10

New Hardware Features in Cisco IOS Release 12.4(11)XW9

New Software Features in Cisco IOS Release 12.4(11)XW9

New Hardware Features in Cisco IOS Release 12.4(11)XW8

New Software Features in Cisco IOS Release 12.4(11)XW8

New Hardware Features in Cisco IOS Release 12.4(11)XW7

New Software Features in Cisco IOS Release 12.4(11)XW7

New Hardware Features in Cisco IOS Release 12.4(11)XW6

New Software Features in Cisco IOS Release 12.4(11)XW6

New Hardware Features in Cisco IOS Release 12.4(11)XW5

New Software Features in Cisco IOS Release 12.4(11)XW5

New Hardware Features in Cisco IOS Release 12.4(11)XW3

New Software Features in Cisco IOS Release 12.4(11)XW3

New Hardware Features in Cisco IOS Release 12.4(11)XW2

New Software Features in Cisco IOS Release 12.4(11)XW2

Cisco Unified Communications Manager Express 4.2

1.
2.
3.

New Hardware Features in Cisco IOS Release 12.4(11)XW1

New Software Features in Cisco IOS Release 12.4(11)XW1

New Hardware Features in Cisco IOS Release 12.4(11)XW

New Software Features in Cisco IOS Release 12.4(11)XW

- Voice Quality Enhancements

Voice Quality Enhancements

New Features in Release 12.4T

Cross-Platform

Release Notes

Limitations and Restrictions

Caveats

-
-
-
-
-
-
-

Open Caveats - Release 12.4(11)XW10

Resolved Caveats - Release 12.4(11)XW10

-

-

  -

  -

  -

could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

This vulnerability does not apply to the Cisco IOS SCP client feature.

Cisco has released free software updates that address this vulnerability.

There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

This advisory is posted at the following link:

http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml.

CSCsu11522

A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS software that can be exploited remotely to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address this vulnerability. There are no workarounds available to mitigate the vulnerability apart from disabling SIP, if the Cisco IOS device does not need to run SIP for VoIP services. However, mitigation techniques are available to help limit exposure to the vulnerability.

This advisory is posted at the following link:

http://www.cisco.com/warp/public/707/cisco-sa-20090325-sip.shtml.

CSCsk64158

Symptoms: 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.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory. This advisory is posted at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml.

CSCsw24700

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.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds that mitigate these vulnerabilities. This advisory is posted at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml

CSCso04657

Symptoms: 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.

`CSCin76666 H.245 listener socket closed before H.245 connection is established.`

Symptom

Conditions

Workaround

`CSCse59336 Three way call conferencing is not working properly.`

CSCsg35148 Interim record is sent with stop-only acct-list from RADIUS.

CSCsj04758 Wrong codec bytes on the SIP leg of ipipgw for SIP--->H323 (g726).

Wrong codec bytes are displayed on the SIP leg of ipipgw for SIP--->H323 interworking.

Work codec bytes of "0" is seen when SIP--->H323 interworking is done when codec g726 codec is configured. Call goes through fine but wrong bytes are displayed.

None.

CSCsj75250 crafted SCTP packet reloads router.

CSCsk40676 C1812 12.4.15.T / certain packet sizes 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.

Disable LZS compression.

CSCsm45113 RIB installs duplicate routes for the same prefix

Further Problem Description: The <CmdBold>clear ip route *<noCmdBold> command can correct the routing table until the next poll of ipRouteTable MIB.

CSCsm49826 c7206VXR/NPE400 reloaded due to bus error running 12.4(15)T2 and T3.

c2691-15(config)#voice service voip

c2691-15(conf-voi-serv)#h323

c2691-15(conf-serv-h323)#no h245 simultaneous-connection-handle

CSCso47738 No Voice Path For SIP to H323 calls.

Gateway sends 200 OK with media direction as SENDRECV for a reINVITE with offer having media direction INACTIVE.

This is seen for the supplementary services when the call is put on HOLD and then RESUMED.

None.

The Watch button is not lit on if no watched phone for this watched DN. Ring back tone is heard when calling to this DN.

No phone, no matter registered or not, is configred with the watched DN.

None.

CSCsq04046 GUI: IOS SYSfeature undefined" error seen on help->about.

CSCsr27960 Traceback observed after configuring credential under sip-ua.

CSCsr78883 Router console displays messages "Data corruption Data Inconsistency.

mls qos cos pass-through dscp

mls qos cos override | cos-value

Further Problem Description:

CSCsu36827 CUE clock does not sync up with the CME using NTP.

CSCsu59847 The Content-Type used by T.37 should use a mutipart subtype of "mixed".

CSCsw50802 Smart Init Fails to recognize HWICs with smart cookie.

CSCsq13348

CSCek52673 Single crafted udp packet reloads router with dhcp server

CSCek71149 Error message when **dir**

dir <archive/system/tmpsys:> **dir nvram/flash/usbtoken0:**

CSCsg42546 Reload when MGCP CRCX has sRTP and V150 params in LCO

CSCsj32422 CBWFQ:Unable to reconfigure the policy map after exceeding the bandwidth

75% in CBWFQ).

Do not exceed the bandwidth while configuring the policy map.

Performing the snmpwalk on the ipRouteTable MIB may cause high CPU and reloads.

This symptom is observed on a router that is running Cisco IOS Release 12.4(13b) or later releases.

Create a view that excludes the ipRouteTable:

snmp-server view cutdown 1.3.6.1.2.1.4.21 exclude

snmp-server view cutdown internet included

snmp-server community <comm> view cutdown RO

CSCsj82622 Crash editing ACL cce_dp_named_db_ip_access_list_impure

message is generated: %ALIGN-1-FATAL: Corrupted program counter pc=0x0 , ra=0x0 , sp=0x66EFB8A0

This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.4(15)T or Release 12.4(15)T1.

There is no workaround.

The following SNMP is incorrectly generated:"%SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full". This issue is affecting the CISCO-MEMORYPOOL-MIB instead.

Occurs on a Cisco 2600 series router running Cisco IOS Release 12.4(11)T3. The router keeps dropping SNMP packets. The log shows that the packets are dropped because of the input queue being full. Although the utilization is sometimes high, this could not be the root cause, as the router keeps dropping packets regardless of the current utilization. Also, the snmp process takes 5-20% of the CPU load.

Exclude ciscoMemoryPoolMIB from your query with the following commands:

snmp-server view public-view ciscoMemoryPoolMIB excluded.

CSCsk94676 dlsw with tbridge, COMMON_FIB-4-FIBIDBMISMATCH

*Jan 29 19:00:50.727: %COMMON_FIB-4-FIBHWIDBMISMATCH: Mis-match between hwidb DLSw Port0 (ifindex 5) and fibhwidb GigabitEthernet2/3 (ifindex 5)-Traceback= 407C7004 407C8A38 407C7CEC 407C7EE4 413C9900 41BCE138 41BCCD54 41BCCFA8 41BCA330 413C0128 413C0114

*Jan 29 19:00:50.727: %COMMON_FIB-4-FIBMISSINGHWIDB: No fibhwidb while initializing fibidb for DLSw Port0 (if_number 5)

-Traceback= 407C83D4 407C8A9C 407C7CEC 407C7EE4 413C9900 41BCE138 41BCCD54 41BCCFA8 41BCA330 413C0128 413C0114

When using DLSw+ together with transparent bridging.

For a workaround, all transparent bridging commands related to can be replaced with DLSW Ethernet redundancy.

i.e.

As global command:

and on the interface:

on the interface replace it with:

A router running Cisco IOS may crash due to watchdog timeout.

Occurs when IP SLA probes are configured and active for a period of 72 weeks. After this much time has passed, polling the rttmon mib for the probe statistics will cause the router to reload. Then the problem will not be seen again for another 72 weeks.

There is no workaround.

Device running 12.4(17.6)T will crash after adding line to an access-list attached to a service policy

There is none.

If the HTTP secure server capability is present, Switch shows the error message "%DATACORRUPTION-1-DATAINCONSISTENCY: copy error" with tracebacks after initializing the supervisor. This error message can be verified in output.

is configured.

Configure The switch functionality is not affected by this error message.The problem is cosmetic.

CSCso09539 ACK not sent to 200 OK from CUE during h323 slowstart -- sip delayed med

Incoming H323 slow start call to CME when forwarded to voicemail in CUE may result in no audio.

This problem was observed when CME did not send ACK to 200 OK response from CUE.

Use H323 Faststart.If incoming H323 calls need to be slow-start for video calls and calls to voicemail need to be faststart, enable H.450 call transfer feature and use two incoming dial-peers:

One H323 dial-peer configured with " "
and H323 slowstart using voice-class h323.

Another H323 dial-peer configured with " " and
H323 faststart using voice-class h323.

CSCsq42134 JPN: 7921 XML Services are displayed as squares

CSCsq44013 View used twice with logging enabled

CSCsq64715 EM login credential could be set to stack junk in error condition

CSCsq67163 IPSLA RTP operation crashes the router

CSCsq74999 SCCP FXS ports connected to FAX machines lock up

CSCsr01058 SPLIT_DNS: Debug msg Forwarding back reply is missing

CSCsr18200 busy tone issue when receiving a 183 Message

CSCsr71715 Call display missing when park or xfer HW conference call

CSCse70333 CFwdAll erroneously reconfigured after disabling night service

CSCsj38755 Ping Fails over ATM interface.

CSCsl26765 DTMF not detected by CUE if I/C call is txfer to ph with CFDWALL to VM

CSCsm23378 DTMF transcoding from rtp-nte to in-band fails for same codec

CSCsm34706 CUBE sends fixed DTMF duration and ignores received H.245 User Input

CSCsm37093 CME 4.1after security is enabled 7970 will register with US locale.

CSCsm64258 ephone-hunt group does NOT present calls to overlaid DNs

CSCsm74560 phone does not look for network locale file for user defined languages

CSCsm88771 CME trunk optimized calls being put on hold automatically

CSCsm89158 7921 does not display call park number while the call is parked

CSCso25982 SIP transfer at connect with No Audio

CSCso26056 SIP Extension unable to transfer at alert to a PSTN number

CSCso27097 One way audio after xferring incoming SIP trunk call with transcoder

CSCso36239 wrong primary-phone observed after re-configure primary-dn of the ephone

CSCso39201 ephone gets into DND mode while in Connected state

CSCso42145 CCME ephone name config result in called number display issue

CSCso45361 High jitter in ringback from CUE

CSCso56824 SCCP OOB-RFC2833 DTMF interworking issue for CME customer

CSCso64585 redundant CallRemoteMultiLine sccp msg to monitor park DN

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

CSCso74656 MG2:device-based BLF shown incorrect status for EM

CSCso78702 7961 IP Phone acct softkey get "no park number available"

CSCso95643 sRTP Package missing in c1861

CSCsi55685- kron removes recurring tclsh cli after first run

occurrence tcl in 1 recurring policy-list tcl ! kron policy-list tcl cli tclsh disk0:hello.tcl!

enter the following configuration commands: kron occurrence tcl in 1 recurring policy-list tcl ! kron policy-list tcl cli tclsh unix:hello.tcl ! create a file on disk0: called hello.tcl with the following contents: puts "hello"

None

CSCsk25697- unprotected buginf may cause cpuhog under repeated udp traffic to 53

A router with DNS server configured may show CPUHOG tracebacks when it receives repeated crafted udp packets to its port 53. Sample for 3800 router: %SYS-3-CPUHOG: Task is running for (40004)msecs, more than (2000)msecs (5/0),process = DNS Server Input. -Traceback=0x60D68CDC 0x6033D984 0x6180E58C FFFFFFA0 3F 4E 60 0x708DFD18 06 FFFFFFFE FFFFFF88 FFFFFFA5 FFFFFFA3 FFFFFF92 FFFFFFA7 FFFFFF8B 7A 3A FFFFFFF5 17 FFFFFF9B FFFFFFC9 FFFFFF9B FFFFFFA2

Router needs to have dns server configured and listen to udp port 53 conf t ip dns server end

Apply rate limit to port 53 to interfaces facing untrusted networks: access-list 100 permit udp any any eq domain access-list 100 deny ip any any interface GigabitEthernet0/0 ip address 10.2.2.2 255.255.255.0 rate-limit input access-group 100 8000 1500 2000 conform-action transmit exceed-action drop.

CSCsl48237- incorrect bounding length in sstrncpy() calls in l2tp files

If a large name string is used when configuring the command "security crypto-profile" under the l2tp-class submode, we could have a buffer overflow which may crash the router.

This problem only occurs if a large name string is used in the "security crypto-profile" command.

There is no workaround.

CSCsl59294- %DATACORRUPTION-1-DATAINCONSISTENCY at caplog_logger_proc

size

filename

size

filename.

CSCsm46227- Router crash with CPUHOG for trunk port monitoring.

```
% Configuration buffer full, can't add command: !
 %Aborting Save. Compress the config, Save it to flash or Free up space on device
```

CSCsk31644 Spurious Access at cmm_crs_proc_tr_call_consult_resp

CSCsk55078 CME 4.2 Diversion Header issue in chained supplementary service

CSCsk22265 CME: 7935 and 7936 Corporate Directory Lookup fails in CME 4.1 and 4.2

CSCsk50911 Need to update the max-ephones range for various platforms

CSCsk25651 ephone-dn removal does not clean up mwi state

CSCsj53899 Remove xlate profile from voice register dn removes from dial-peer

CSCsj93762 Resume fails after HOLD for SIP phones regist with voice-class codec

CSCsj81363 FRU incorrect and Carrier Set empty on wireless B sku platforms

CSCsk42889 SIP call xfer to voicemail fails with DNS Query failed error

CSCsk58359 Update max sip phone range for various platform

CSCse14595 call may be connected while being cfna to an PSTN call

CSCsk35315 CME: calledName= displayed garbled characters

display name information; for example an inbound facility message for Advice of Charge (AOC) may trigger this problem.

These messages can be seen on the gateway through the use of debug isdn q931. Caution should be taken when enabling any debugs on a production router/gateway as it can impact performance. Make sure as a minimum to disable console logging on the IOS device before enabling any debug. This issue does not have an impact to the operation or performance of the gateway nor phone.

Contact the ISDN service provider to determine if the facility messages causing this problem can be disabled.

CSCsk16153 Modem won't be disconnected on exit

Modem connection is still active on exit.

After "exit" from modem session.

There is no workaround.

CSCsk73035 dtmf stop working if using connection plar opx immediate on fxo port

dtmf stop working if using connection plar opx immediate on fxo port.

Cu is running 124-11.XW on uc520. the dtmf does not work in the following call flow:

```
pstn--fxo---gw--sip--cue AA

If removing "immediate" from the following config,
the dtmf works.

voice-port 0/1/0
connection plar opx immediate 111
caller-id enable
```

CSCsk46424 Authentication fails on main dot11 interface when xconnect configured

CSCsk52683 System crashed when wireless client is trying to associate with AP

CSCsk17498 Per Port Storm-Control is broken

CSCsj88854 Router crashes when a call is made from Remote Phone registered to CUCME

CSCsj02456 HTTP PUT operation using copy command failed

CSCsk83795 call may be disconnected when resetting other ephone

CSCsj14565 ACL = deny; sa request ignored when crypto local-address is dynamic

For example:

```
crypto map mycryptomap local-address Dialer0
interface Dialer0
 ip address negotiated
```

CSCsk74181 SIP DO-DO - Basic Fax call fails

CSCsl04993 uc520 devices does not get reload via SNMP

CSCsj56438 Crafted EAP Response Identity packet may cause device to reload

* Wireless EAP - CSCsj56438
* Wired EAP - CSCsb45696 and CSCsc55249

CSCsk66907 %SYS-3-CPUHOG: due to Skinny MOH Server process

%SYS-3-CPUHOG: Task is running for (xxx)msecs, more than (xxx)msecs (xxxxxx),process = Skinny MOH Server.x

CSCsi60392 CME does not send SIP NOTIFY DTMF to CUE-AA after txfer from CUE-VM

CSCsl12443 CME: TNP phones may experience one way audio

OpenReceiveChannelAck status orcError on socket

CSCsj38652 Freddo DTMF/cptone issues for Taiwan, Hong Kong, Singapore Compliance

CSCsk83813 sip call will pick up the wrong codec type from voice class codec

```
voice class codec 1
      codec preference 1 g729r8
      codec preference 2 g711ulaw

dial-peer voice 9191916 pots
 description #1/1:16#0# INUSE 163
 destination-pattern 19900001429191916
 port 1/1:16

dial-peer voice 555 voip
 rtp payload-type lmr-tone 107
 rtp payload-type nte-tone 108
 voice-class codec 1
 session protocol sipv2
 incoming called-number.
 dtmf-relay rtp-nte
 no vad

Using 2811
Cisco IOS versions: 12.4(17.4)PI1b and 12.4(17.4)PI1a
```

CSCsk63037 CME 4.2 has broken caller ID feature

CSCsk95708 10 to 30 sec delay in starting media in secure meet-me conference

CSCsk42180 Few Objects of CISCO-LICENSE-MGMT-MIB giving wrong values during SNMP wa

CSCsj94818 C877: ADSL2+ AnnexM: PVC goes to INAC after QoS is applied

CSCsk06443 SIP TGW sends 183 response even though no response from ISDN

CSCsk36600 Router crashes when ExtACL has mixed of tcp host and tcp net with QoS

CSCsj80906 Router crashes on changing ACL linked to service policy

CSCsl17037 CME: Local Directory Issue

CSCsl04115 CM call to CME when Put on Hold, CME Hears FastBusy instead of TOH

IPPhoneA---CM---H323---CME---IpPhoneB

- Phone A calls Phone B
- Phone A puts Phone B on Hold.
- Instead of playing Tone On Hold, Phone B user hears a fast busy tone.

CSCsk72582 Call in B-ACD drops if answered after hunting second time round

CSCsj97535 BACD functionality broken on freddo

CSCsi50316 fix linux builds for rdo tools

CSCsh74385 EEM fails to register with the redundancy framework (RF)

```
nms-7206vxr(config)#event manager applet testapp
                                 ?

  cli           CLI event
  counter       Counter event
  interface     Interface event
  ioswdsysmon   IOS WDSysMon event
  none          Manually run policy event
  oir           OIR event
  resource      Resource event
  snmp          SNMP event
  syslog        Syslog event
  timer         Timer event
  track         Tracking object event

nms-7206vxr(config-applet)#
```

CSCsj25470 EEM hostnames over 20 characters causes CLI actions to hang

Multiple voice-related vulnerabilities are identified in Cisco IOS

Multiple voice-related vulnerabilities are identified in Cisco IOS

CSCek78645 Analog phones cannot register with CME

CSCsj29857 xfer to ICD failed after conference AA

CSCsi13312 Authentication fails and unable to login to a factory fresh router

http://www.cisco.com/en/US/ts/fn/620/fn62758.html

CSCsg62638 CPU usage reaches 99% after nmap scan on port 53

CSCsi56172 CME 4.1 IP phone dropped when trying to complete hardware conference

CSCsi58842 CME: 7960+7914 display select line when conference IP phone

CSCec12299

CSCsi01470

CSCek61570 Trunk dn stuck in seize/seize state and does not recover

CSCek67866 xcodemsp.c Static Analysis Found Issue

CSCek70830 $$TS: cme crashed during call to ICD routept running 124-11.3.4.PIA1

CSCsg36112 In xcoding, SCCP sessions not cleared immediately after abrupt call end

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

CSCsg69022 c1700 router crash @ nv_write_internal

CSCsh65321 Phones fail to do secure authentication in 12.4(12.12)PI6

CSCsh73754 SmartPorts: PC connected to an IP phone cannot connect to WAN

CSCsh80217 No Audio Path after REFER from xto to xee in a Meetingplace scenario

CSCsh81876 Traceback & crash if guest mode and multiple vlans

CSCsh89887 One way voice path with h/w conference on ephone-dn w/o preference 0

CSCsi03314 test ecdsa display-stats command not displaying output

CSCsi04538 Router crash with memory corruption when configure cert-upgrade auth mod

CSCsi09530 CME SIP phone failed to register because of authenticate register

Further Problem Description

Symptom

Conditions

Workaround

Symptom

Conditions

Workaround

Problem Description

Symptom

1.

2.

Root Cause **Xfering_SetupDone()**

```
cmm_crs_proc_tr_call_trans_req()
```

Conditions

Workaround

Additional References

Release-Specific Documents

- *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

Notices

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