Record ID: VID10493-0005-ACMR

CCEVS Approved Assurance Continuity Maintenance Report

Product:	Cisco 5915 Embedded Services Router (ESR) Running IOS Version 15.2(3)
EAL:	2 augmented with ALC_FLR.2 and ALC_DVS.1
Date of Activity:	6 May 2013
References:	Common Criteria Evaluation and Validation Scheme - Assurance Continuity: Guidance for Maintenance and Re-evaluation, Version 2.0, September 8, 2008 Impact Analysis Report for Common Criteria Assurance Maintenance Update of Cisco 5915 ESR Running IOS Version 15.2(2) to Cisco 5915 ESR Running IOS Version 15.2(3), Version 1.2, EDCS-1217891, May 2, 2013
Documentation Updated:	Cisco 5915 Embedded Services Router Security Target, Revision 1.0, 10 January 2013 Cisco 5915 Embedded Services Router Common Criteria Operational User Guidance and Preparative Procedures, Version 0.05, 11 January 2013 Cisco C5915 15.2(3) GC Common Criteria Test Results, 8 October 2912 Configuration Management, Lifecycle and Delivery Procedures for Cisco 5915 Series Embedded Services Router, Version 1.3, EDCS-1223210, January 10, 2013

I. Introduction

On 14 February 2013, Cisco submitted an Impact Analysis Report (IAR) for the Cisco 5915 Embedded Services Router. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme - Assurance Continuity: Guidance for Maintenance and Re-evaluation, Version 2.0 , September 8, 2008. In accordance with those requirements, the IAR describes the changes made to the yet to be certified TOE, the evidence updated as a result of the changes, and the security impact of the changes.

II. Changes to the TOE

The primary reason for this Assurance Continuity Maintenance activity on the Cisco 5915 ESR is to address bugs in the version 15.2(2) of the software and update the version number to 15.2(3).

Summary of Changes

5915 ESR bug fixes are tracked within Cisco's distributed defect tracking system (DDTS). Each bug, whether identified by a customer or within Cisco is tracked within DDTS, and given a DDTS identifier.

Each DDTS report contains a brief "headline" and more detailed discussion of the problem and the resolution. The vendor examined each of the detailed DDTS reports and drafted the "brief description" found in the tables below by referencing the DDTS headline and the report details. The vendor made the determination of which category was applicable for each report by:

1. Examining the "headline" and immediately classifying those that involved items that were excluded from the TOE or had no security relevance (such as grammatical corrections to help files) into the "Minor Changes with Little or No Security Relevance" category. This ruled out more than half of the reports.
2. For the remaining items, the details of the report were examined, including what the implications of the noted issue was, and what changes were required. Fields such as the report summary, how the report was found, workarounds, and attachments that showed device captures, test results, and configurations applicable to the report were examined to determine security relevance. Once again, the vendor was able to classify a large number of reports into the "Minor Changes with Little or No Security Relevance" category as they were unrelated to the TSC. (See Section 5.2 under "Examples of minor bug fixes that are not related to the TSC" for specific groups of reports that were classified in this manner.)
3. The items that were found to be related to the TSC were noted as such and then the vendor examined them in detail to determine whether they involved a change that made the TSC behave as advertised or involved major changes that jeopardized the TSC enforcement. The vendor also determined which TOE Security Function was applicable for each of these reports.

Each of the fixes to the 5915 ESR fall into the following categorizations:

- Minor Changes with Little or No Security Relevance: These changes may be related to the TSC in some way, though may or may not relate directly to an SFR defined within the ST.
- Minor Changes with Some Security Relevance: These changes relate to the TSC in some way though the affect of the change is only to ensure the TOE functions as expected, and does not add or detract from the stated requirements in the ST. Therefore, changes in this category result in no adverse affect to the assurance baseline.

None of the fixes to the 5915 ESR fall into the following category:

- Major Changes: These changes can be directly related to some SFR, and modify how the TOE meets that SFR such that the TSS or design documents are no longer accurate.

Non-security Relevant Hardware

Minor Changes with Little or No Security Relevance

The fixes listed in the subsections and tables below do not directly apply to the TSC, and fall out of the scope of evaluated functionality. They are grouped based on rationale.

Non-Security Relevant Commands and Options

The Command Line Interface of the TOE includes many commands that have no security relevance, and are not TSFIs, or non security relevant parameters. All updates to the TOE that dealt with these commands were not applicable to the TSF. This affects the following fix entries:

Table 1 Minor Changes: Non-Security Relevant Commands

Identifier	Component	Description of the Issue
CSCts47776	media-mon	router crashes due to performance monitor database debug
CSCts56044	flexible-netflow	MF:YAP: FNF Top Talkers: crash with complex aggregate / sort
CSCts97925	fib	IPv6 pings fail within the same VRF through global next hop
CSCts98336	ipsec-ikev2	unconfiguring ikev2 profile is causing a crash
CSCts74982	media-mon	Collision when creating monitor object, Unable to create monitor object
CSCts89785	parser	GENERAL_TIME needs addition to support WNBU commands
CSCtt16051	smartoperations	Malformed Smart Install message causes device reload
CSCtt17904	mediatrace	Parser ambiguity for exec mode mediatrace commands
CSCtt45536	nbar	"FlowVar- Chunk malloc failed" msgs seen with mix of IPv4 & IPv6 traffic
CSCtu20233	ntp	Remove the Cli support for telecom solutions driver
CSCty44304	medianet-metadata	Feature ID for metadata IPv6
CSCty45319	c5915	Incorporate Freescale recommendation for Data Cache Flush
CSCty59259	c3pl	ONE-P PSP: Change PSP feature location after classification
CSCty60866	c5915	Enable GDB in C5915 Xspace Images
CSCty61201	c5915	Fix inclusion of subsystems in c5915 entbase

Grammar, Help, and Documentation Updates

Updates to the syntax, spelling, and grammar used in a command that have no bearing on the security relevance of the command, or that restore the command to its functionality described in the evaluation documentation do not interfere with the TSF. Updates to the documentation (command references and configuration guides) have no effect on the TSF, as the updated guides are part of the new evaluation record. Updates to the help messages displayed for commands have no effect on the TSF. Updates to comments within the code have no effect on the TSF. All updates to the TOE that dealt with these scenarios were not applicable to the TSF. This affects the following fix entries:

Table 2 **Minor Changes: Grammar**

Identifier	Component	Description of the Issue
CSCtr55973	ldap	Spaces in bind authenticate string

Changes for Memory Leaks

Changes to the code that are to correct memory leaks and out of bounds references to buffers simply correct defects in the code and have no affect on the TSF. All updates to the TOE that dealt with these scenarios were not applicable to the TSF. This affects the following fix entries:

Table 3 Minor Changes: Changes for Memory Leaks

Identifier	Component	Description of the Issue
CSCts28761	isis	Crash while isis reconfig and issuing "sh isis data" in parallel session
CSCts44718	flexible-netflow	crash found on fnf_cache_remove_from_free_list
CSCts60981	common-flow-table	NMI Watchdog timeout crash at be_cft_ipv6_get_next_header
CSCtt21979	rsps-time-rptr	Processor Pool Memory leak in IP SLA Responder with IPv6 Probes
CSCtt26074	rsps-time-rptr	Huge Memory leak with IPSLAs XOS Even process at slaSocketAddContext
CSCtw67283	common-flow-table	Unexpected exception to CPU in action_add_standard_global during traffic
CSCtw50141	ldap	Incremental leaks at __be_ber_get_stringa pointing to LDAP Process
CSCtt94986	isis	CLNS L1 addresses are not Leaked to L2 (with only one area address)

Telnet, SNMP, or XML Management

Use of Telnet, SNMP, or XML for management, which are excluded in the ST, would take the TOE out of the evaluated configuration. All updates to the TOE that dealt with support of SNMP or XML management were not applicable to the TSF. This affects the following fix entries:

Table 4 Minor Changes: XML and SNMP Management

Identifier	Component	Description of the Issue
CSCts03996	ipsec-getvpn	SNMP query cgmGdoiKsKekRemainingLifetime returns value wrong

Virtual Private Networks

Virtual Private Network (VPN) functionality was included in the TOE. Some updates to the TOE that dealt with implementation of VPNs are not applicable to the TSF. This affects the following fix entries:

Table 5: Minor Changes: Virtual Private Networks

Identifier	Component	Description of the Issue	Rationale
CSCts98336	ipsec-ikev2	unconfiguring ikev2 profile is causing a crash	Does not affect the TOE because the TOE will be configured for ikev1 while in the evaluated configuration per FCS_IPSEC_EXT.1.

Switching and Routing Protocols

No security claims were made with respect to routing & switching protocols in the ST. All updates to the TOE that dealt with support of these routing and switching protocols were not applicable to the TSF. This affects the following fix entries:

Table 6 Minor Changes: Switching and Routing Protocols

Identifier	Component	Description of the Issue
CSCts19788	ospf	crash while show ospf database
CSCtu28990	fib	RLS10.2:RP crash observed @SYS-6-STACKLOW: Stack for process XDR mcast
CSCtu76678	bgp	Extreme rare crash when a bgp neighbor is unconfigured
CSCtw45055	bgp	BGP DN: Crash in BGP Scheduler due to freed bgp neighbor
CSCtx29557	fib	standby crash @ fib_fib_src_interface_sb_init
CSCto56052	mpls-mfi	MPLS Forwarding not working on PPPoA Dialer Interface
CSCto61736	nbar	PACKETS ARE NOT CEF SWITCHED CORRECTLY when NAT is removed
CSCtq59923	ospf	OSPF Routes in rib point to down interface
CSCtq74449	ppp	Ping over PPPoA session fails when Dialer is shut and removed from shut
CSCtr00216	eigrp	MF:EIGRP vnet commands do not sync to standby in SSO mode as expected
CSCtr36399	ribinfra	TB ipc_notify_session on the new active RP console after SSO SW
CSCtr44782	mpls-mfi	Eompls Vc's not taking Tunnel Path when issued oir with latest xe35 imag
CSCtr47642	bgp	BGP_DP: Bestpath selection takes too long in certain condition
CSCtr55689	ipsec-switching	IPv6 FlexVPN:Tracebacks and malloc error at interrupt level
CSCtr56988	ppp	ALIGN-3-SPURIOUS: Spurious memory

		access@pppatm_dialer_shutdown_vaccess
CSCtr69144	bgp	distance change for MBGP doesn't affect
CSCtr69607	nbar	Enabling PD and FNF over 32 subinterface.
CSCtr88739	os	radix tree version walk can skip some eligible nodes
CSCtr98409	eigrp	TB & CPUHOG msg on enabling EIGRPv6 on 10th VRF intf in standalone
CSCts12296	ppp	RFC4638 PPP-Max-Payload implementation(backward-compatibility) broken
CSCts16021	eigrp	Not all services advertised between EIGRP SAF peers
CSCts21080	idb	Tracebacks on standby at __be_swidb_if_index_link_identity
CSCts33379	idb	Tunnel interface is down if the tunnel source interface is recreated
CSCts27042	ipmulticast	Bidir DF election causes traffic duplication
CSCts38022	eigrp	EIGRP loose redistributed static route when peer also redsist same route
CSCts45838	ppp	Harden PPPoE tag processing code to ignore invalid tags.
CSCts50099	fib	'show ipv6 traffic' only counts IPv6 process-switched traffic
CSCts55371	ospf	LSAs are not flooded to the peers.
CSCts55461	flexible-netflow	FNF normal monitor with default values does not age or export entries
CSCts61660	flexible-netflow	Default value for cache entries is wrong
CSCts63501	mpls-mfi	Explicit Null Configuration, in a *not EOS* case is set to Dropa
CSCts64539	bgp	BGP Marks Next HOP inaccessible with ip vrf next-hop feature used.
CSCts66394	fib	Traceback seen @ fib_assert_assertion_failed while booting the image
CSCts69204	ppp	PPPoE Sessions Disappear after RPSO
CSCts88520	flexible-netflow	FNF NOVA: Fix timestamp and fnf_mon_get_max_size problems
CSCtt02313	eigrp	PfR: Uncontrol TC due to Exit Mismatch
CSCtt12278	flexible-netflow	Edison: Fix and remove incorrect CLI for Katana
CSCtt12580	flexible-netflow	Cannot config FNF on a vlan before a vlan is configured/created.
CSCtt17785	eigrp	ASR doesn't exchange routes with ASA, reports ASA as version 0.0/0.0
CSCtt17879	bgp	BGP backdoor command is not working
CSCtt18689	nbar	SPA goes offline with AVC config on physical interface
CSCtt19532	flexible-netflow	FNF NOVA: Fixes to support FNF over SSID for WNBU
CSCtt20427	bgp	PE with additional-path install does not send VPNv4 updates
CSCtt22166	flexible-netflow	FNF NOVA: Stop getting platform flow_def before monitor attach
CSCtt35936	eigrp	RLS3.4 EIGRP route updates are not sent to DMVPN spokes
CSCtt37156	eigrp	multicast neighbor is not shown in"show eigrp service-family ipv6 neigh"
CSCtt43844	flexible-netflow	Got CPUHOG Traceback after do ISSU with 500 AVC conifg
CSCtt44051	fib	Provide HW-API capability to disable prefix based accounting modes
CSCtu00406	fib	Cannot ping local ipv6 intf in next-hop vrf using vrf import/export leak
CSCtt70514	flexible-netflow	FNF NG3K -exporter binding failing on reload or incomplete

		export config
CSCtt96115	flexible-netflow	FNF NOVA: Fix coverity warnings
CSCtu05300	flexible-netflow	FNF NOVA: Fix SPI messages to follow HA model
CSCtu07645	bgp	Unextpected "return" in the Inter-Cluster RR best-external code flow
CSCtu12135	flexible-netflow	FNF NOVA: Assert in fnf_epm_ssid_init() after sync with flo_dsbu7_ng3k
CSCtu16452	flexible-netflow	FNF query ssid name from ifid subblock database using ssid iif-id
CSCtu21124	flexible-netflow	FNF NOVA: SSID Bind can be sent to FFM before Monitor with flow record
CSCtu21457	bgp	cnma1b: BGP unable to install gwcache
CSCtu41137	fib	IOSD Core@fib_table_find_exact_match while unconfig tunnel int
CSCtu43731	flexible-netflow	Watchdog fires taking down RP on ISSU event with 4000 DVTI sessions
CSCtu80224	bgp	BGP sets next-hop for redistributed recursive static routes to itself
CSCtu92891	flexible-netflow	Sampler creation can cause CPU Hog
CSCtu92987	flexible-netflow	FNF NOVA: Fix FNF Observability in Nova code
CSCtu93059	flexible-netflow	FNF NOVA: Fix FNF Observability in IOS code
CSCtw13668	rsps-time-rptr	MF: IPSLA VO rapid config-unconfig sequence causes standby reload
CSCtw62514	ospf	OSPFv3: default hello/dead interval incorrect for P2MP
CSCtx06755	eigrp	EIGRPv6 NSF status never leaves in progress with no NSF peer
CSCtx20604	ospf	Build breakage in routing@(rel4)1.4.3
CSCtu09837	parser	XML-PI: BGP config partition is malformed
CSCtt55925	ip	multicast and pim and bsr advertisements fail over unnumbered ppp link
CSCtt94243	parser	Raise the ECI decoder length limit
CSCtu13300	nbar	PI17:Some pdl-based protocols fails to classify for IPv6 traffic flow.
CSCtu33956	ppp	Dialer with PPP encap when DSL is WAN interface, L2PT not working
CSCtw70352	nbar	Kaaza2 protocol activation was failing on interface
CSCtw76044	ipmulticast	Need registery to get igmp_idb info for MLD interface
CSCtw76759	nbar	Stile simulator build fails due to XOS files missing
CSCtw78343	rsps-time-rptr	rttMonApplSupportedProtocols table missing on 151-4.M1
CSCtw78456	c5940	C5940 ENTITY-MIB missing instances
CSCtw88094	rsps-time-rptr	MF:Standby reload due to line by line sync failure upon sch ipsla sessio
CSCtw99290	mcast-infra	ASR1K:v6 mcast channel zapping and show run in a loop modifies confg
CSCty48755	ipmux	Unit Train: Packet loss detected at low levels of bi-directional traffic
CSCty48872	ipmux	Unit Train: IPv6 full superframes not mux'ed over tunnel interface
CSCty49191	ipmux	Unit Train: Policy CLI commands are not always working properly

CSCtz44095	ipmux	Unit Train: IPv6 Mux Packet loss / counters wrong over encrypted intf
CSCtz47607	ipmux	Unit Train: Tracebacks seen when sending IPv6 full superframes over CEF
CSCtz56717	ipmux	Unit Train: IPv6 full superframes not transmitted over tunnel interface
CSCtz81020	vmi	DLEP: Ping fails after DLEP neighbor flap

Availability

Availability was not part of the TSF claims for the TOE. All updates to the TOE that dealt with implementation of failover for high availability were not applicable to the TSF. This affects the following fix entries:

Table 7: Minor Changes: Availability

Identifier	Component	Description of the Issue
CSCsw96543	ha-issu-infra	Sierra : Crash at 'issu_xmit_transform' during infra testing
CSCtb36677	ha-issu-infra	Router crashes giving TB @ issu_register when MDEBUG is enabled for blob
CSCtn07696	ftp	6506-E/Sup720 crash related to SYS-3-URLWRITEFAIL: and TCP-2-INVALIDTCB
CSCts01653	media-mon	router crash or spurious memory access on video monitoring router
CSCts69973	ipsec-dmvpn	Spoke with 100 tunnels crashed at "nhrp_process_delayed..."
CSCts72164	bgp	Router crashes due to Segmentation fault in BGP I/O
CSCts90043	common-flow-table	Router crash continuously every 10 minutes at fmd_free_fo_cb
CSCtt03100	xconnect	Router crashes with xconnect config
CSCtt07525	nhrp	Flex: Crash on remote spoke when clearing NHRP locally.
CSCty36533	ipmux	Unit Train: Router crashed running bi-directional IPv6 traffic
CSCty51988	ipmux	Unit Train: Router crashes when receiving malformed superframes
CSCty77889	ipmux	Unit Train: Router crash on intf shut with "no singlepacket" IPv6 data
CSCtz07312	c5915	Crash while performing factory default
CSCtz69612	ipmux	Unit Train: Router crash after removing IPv6 address from mux interface
CSCsq08000	ha-issu-infra	Call Home Process consuming 616K more W2 vs. W1 on Acive RP - Non Blob
CSCsr92267	ha-issu-infra	Original monolith code for X-Matrix lookup for Cat6k never committed
CSCsu68557	ha-issu-infra	ISSU debug for C2W2: NEGO_NOT_FINISHED

CSCsy19491	ha-issu-infra	12.2(32ISSU-3-ERP_AGENT_SEND_MSG seen when the sup is power cycled twice
CSCsy70534	ha-issu-infra	ISSU Clients 7200 and 7201 does not allow Matrix Creation in 52.SG
CSCsy97510	ha-issu-infra	add platform overwrite of image name comparison result
CSCta56937	ha-issu-infra	Standby switch is reset because %ISSU-3-JID: Failed to get the JID
CSCtb16965	redundancy-rf	NG3K: HA Bringup
CSCtb68626	ha-issu-infra	ISSU: performance of issu_xmit_transform
CSCtc63598	ha-issu-infra	cnh-sy:client_entity_sending_process TB seen during SSO
CSCti03487	ha-issu-infra	Fix SA warnings in issu@(rel_3)
CSCtq97585	parser	TS:Shell triggers not executed right after switch over
CSCtr15141	igmp	IOS General Query max response code is not following IGMPv3 RFC
CSCts25846	parser	All ST activation failed once hit 'shell execution failed'
CSCts31111	cpu	c880 fails to generate coredump : Watchdog timeout exception
CSCts32900	ipsec-core	%PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT@__be_crypto_allocate_short_handle
CSCts34825	ipmulticast	High cpu seen for Mwheel Process on the latest mcp dev image
CSCts67561	ipsec-core	asr1k:router hangs for 2 min if "clear crypto gdoi" on gm
CSCts71248	parser	MF:Even after wr mem, upon reload with new img, Entserv chnges to Lanbas
CSCts76410	ipsec-vti	VTI: tunnel interface stays up/down even with active SA and socket.
CSCts85459	ipsec-core	C881GW : On Reload, cellular int won't negotiate if crypto map applied
CSCtt23038	flexible-netflow	IOSD core @flow_lock_lock when issuing show command during HA tests
CSCtt36513	ipsec-core	FlexVPN : ASR(Server) reload at process IPSec key engine
CSCty32479	ipmux	Unit Train: Router crashed after shutdown of IPv6 mux interface
CSCtw45592	ntp	CLI "NTP Server <dns name>" - does not get synced to standby
CSCty70972	ipmux	Unit Train: Add feature-id for IPv4 IPMux input feature processing

System Load Testing

The TSF makes no claims about throughput rates; therefore system load testing and updates made because of load testing do not affect the TSF. This affects the following fix entries:

Table 8: Minor Changes: System Load Testing

Identifier	Component	Description of the Issue

CSCtq79382	rsps-time-rptr	rsps-time-rptr
CSCtr62521	config-sync	%ERROR: Standby doesn't support, while re-configuring deleted atm subif
CSCtr86950	flexible-netflow	CPU HOG with FP reload for FNF
CSCts60398	rsps-time-rptr	assert@/cisco.comp/parser/src/parser_actions.c:2147:koa_walk_option(): "
CSCts67465	rsps-time-rptr	MF:IPSLA VO: Reconfiguration of frequency value causes standby to reload
CSCts70790	bgp	BGP default-originate for VRF neighbor does not work after link flap
CSCts89761	media-mon	Allow platforms to restrict modify of attached MMON Policy:Comp changes
CSCts65790	rsps-time-rptr	MF:Duplicate 4-tuple Video probe cause Standby to reset
CSCtt15963	media-mon	MMON capability is not set correctly if MIN_VALUE and MAX_VALUE are same
CSCts69368	rsps-time-rptr	timeout trap is not displayed in ip sla engine 3
CSCtt04371	ntp	Need to change the default setting in NTPv4 for faster sync
CSCtt18206	rsps-time-rptr	K10 Medianet: IP SLA IPVSC Sender Transmitted cntr always 0 after reload
CSCtt27575	rsps-time-rptr	Reserve dsp does not show up in the running config
CSCtt44468	rsps-time-rptr	Set IP SLA Video Config fails with SNMP
CSCtu03690	rsps-time-rptr	emulate source and dscp CLI broken with no reserve dsp for ip sla video

QoS

TSF makes no claims about Quality of Service (QoS) functionality. All updates to the TOE that dealt with implementation of QoS were not applicable to the TSF. This affects the following fix entries:

Table 9**: Minor Changes: QoS**

Identifier	Component	Description of the Issue
CSCtq79382	rsps-time-rptr	rsps-time-rptr
CSCtr62521	config-sync	%ERROR: Standby doesn't support, while re-configuring deleted atm subif
CSCtr86950	flexible-netflow	CPU HOG with FP reload for FNF
CSCts60398	rsps-time-rptr	assert@/cisco.comp/parser/src/parser_actions.c:2147:koa_walk_option(): "
CSCts67465	rsps-time-rptr	MF:IPSLA VO: Reconfiguration of frequency value causes standby to reload
CSCts70790	bgp	BGP default-originate for VRF neighbor does not work after link flap
CSCts89761	media-mon	Allow platforms to restrict modify of attached MMON Policy:Comp changes

Voice Capabilities

TSF makes no claims about Voice functionality. All updates to the TOE that dealt with implementation of Voice applications were not applicable to the TSF. This affects the following fix entries:

Table 10**: Minor Changes: Voice**

Identifier	Component	Description of Issue
CSCtq61590	idb	Cellular interface status not shows "spoofing" instead it shows "up"

DHCP Server

TSF makes no claims about DHCP server functionality. All updates to the TOE that dealt with DHCP server functionality were not applicable to the TSF. This affects the following fix entries:

Table 11**: Minor Changes: DHCP Server**

Identifier	Component	Description of Issue Causing Change
CSCtj48387	dhcp	Crash on ESR due to corrupt values passed from DHCP component to doprnt

Compiler Tool Changes

Changes to the compiler that is used, and changes to make compilation successful have no affect on the TSF. All updates to the TOE that dealt with these scenarios were not applicable to the TSF. This affects the following fix entries:

Table 12**: Minor Changes: Compiler Tool Changes**

Identifier	Component	Description of Issue Causing Change
CSCtr92315	ha-issu-infra	gcc.c4.2.1 compilation errors

Minor Changes with Some Security Relevance

Table 13: Minor Changes with Some Security Relevance: 5915 ESR Switches

Identifier	Component	Headline	Security Audit	Cryptographic support	Traffic Filtering ACLs	Identification and Authentication	Secure Management	Protection of the TSF	TOE Access	Trusted Path/Channels	Intrusion Prevention Services
CSCtr87740	ipsec-switching	Crash seen at crypto_check_acl due to freed postdecrypt_check ACL		X							
CSCtt11210	pki	PKI - IKE cert-req contains issuer-name instead of subject-name of SubCA		X							
CSCtt18020	ssh	crash cleaning up ssh session		X				X			
CSCtn64214	ssh	WSMA SSH does not respond to request even though debugging shows success		X							
CSCto16082	ssh	Unable to remove server confiurations under ssh configs		X							
CSCtq36976	pas-ipsec	VSA breaks BFD when crypto map on same interface		X							
CSCtq38731	parser	config mode exclusive not found in 15.0 ,only option is conf register					X				
CSCtr28510	ipsec-core	For the Antireplay feature,OVERALL WINDOW SIZE check for all Sa's failed		X							
CSCtr73288	parser	After a session timeout, standby console allows commands					X				
CSCts38429	ipsec-isakmp	Cisco IOS Software IKE DoS vulnerability		X							
CSCto93880	aaa	IPv4 Enable authentication failed with tacacs				X					
CSCts43987	esm	Rollback Aborts under "(config)#default logging esm"					X				
CSCts48211	ipsec-ikev2	"show crypto sess detail" shows junk phase1_id for ikev2 session		X							
CSCts56059	flexible-netflow	Top N Talkers:filter ipv4 TOS not working					X				
CSCts63176	ipsec-vti	IPSec dVTI uncloning issues			X						

Identifier	Component	Headline	Security Audit	Cryptographic support	Traffic Filtering ACLs	Identification and Authentication	Secure Management	Protection of the TSF	TOE Access	Trusted Path/Channels	Intrusion Prevention Services
CSCtt04376	aaa	Username with access-class option fails AAA authorization with RADIUS				X					
CSCtt16261	ipsec-core	V6 CM: IPSec sessions cannot stay up			X					X	
CSCtt18697	netconf	Netconf server should warn client about missing cap and unexpected hello					X				
CSCtt28703	pki	CA trustpoint anchor does not work on isakmp profile		X							
CSCtt29885	parser	Interactive commands do not work on the standby					X				
CSCtx44060	ipsec-core	Flexvpn spoke to spoke tunnel doesn't come up			X						
CSCtx90299	ipsec-core	XE36 DMVPN: all IPSec sessions torn down never came back after link flap			X						
CSCtw45332	mpls-vpn	VPNoMGRE after SSO, second traffic drop for 80s due to label change			X						
CSCtw58586	ipsec-vti	default ikev2 profile should be anchored to the default ipsec profile		X							
CSCto71671	aaa	Radius source port extended does not always increase udp src port				X					
CSCtw57751	aaa	Tacacs enable authentication on IPv6				X					

Major Changes

None.

Vulnerability Analysis

A search was done of http://www.securityfocus.com/vulnerabilities for vulnerabilities related to the TOE using the following key words:

Cisco -> IOS -> 15.2(2)GC and there were no vulnerabilities found.

A second search was done of http://tools.cisco.com/security/center/publicationListing for vulnerabilities related to the TOE using the following key words and no vulnerabilities were found:

IOS 15.2(2)GC - IOS 15.2(3)GC, ESR 5915

III. Analysis and Testing

The test cases used for the original evaluation were successfully re-run on the updated software. The vendor analysis shown in Section II supports the conclusion that the bug fixes resulted in only minor security affects to the evaluated configuration.

IV. Conclusion

This maintenance activity covers the assessment of the affects of the changes to the Cisco 5915 Embedded Services Router software with respect to the evaluated product. The listed changes to the Cisco 5915 software show that only minor security affects are noted. Therefore the conclusion is that the changes are acceptable under the assurance maintenance program.

In addition, it is important for the user of this product to review the original Validation Report Sections 4 and 10 and the new ST to understand any limitations on the evaluated configuration.