Release Notes for Cisco Security MARS Appliance 5.2.4

Revised: May 29, 2007, OL-13016-01

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

These release notes are for use with the Cisco Security Monitoring, Analysis, and Response System (MARS), Version 5.2.4 running on any Local Controller or on any Global Controller. They provide the following information:

Introduction

Version 5.2.4 is now available as an initial software release in support of the second generation MARS Appliance models as identified in Supported Hardware, page 2.

Caution Do not attempt to apply 5.2.x versions to MARS 20, 20R, 50, 110, 110e, 200, GC, or GCR models. It is supported exclusively by the models listed in Supported Hardware, page 2.

Registered SMARTnet users under the can obtain version 5.2.4 from the Cisco support website at:

http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars

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

Supported Hardware

Cisco Security MARS Version 5.2.4 supports the following Cisco Security MARS Appliance models:

Local Controller Appliances

- Cisco Security MARS 110 (CS-MARS-110-K9)
- Cisco Security MARS 110R (CS-MARS-110R-K9)
- Cisco Security MARS 210 (CS-MARS-210-K9)

Global Controller Appliances

- Cisco Security MARS GC2 (CS-MARS-GC2-K9)

New Features

In addition to resolved caveats, this release includes the following new features:

- Miscellaneous Changes and Enhancements, page 2
- New Vendor Signatures, page 3

Miscellaneous Changes and Enhancements

The following changes and enhancements exist in 5.2.4:

- **Support for new hardware model.s.** Cisco Security MARS Version 5.2.4 supports the new hardware models as defined in Supported Hardware, page 2.
- **New license scheme for upgrade.** The license scheme now supports a software only license upgrade from restricted models, such as the 110R, to full versions, such as the 110. This feature allows you to gradually grow your MARS deployment without costly hardware upgrades, and it protects your investment in time, configuration, and existing hardware.
- **Support for Extended Daylight Savings Time.** On March 11, 2007, the United States will adjust to Daylight Saving Time (DST) three weeks earlier than previous years and will end one week later on November 4, 2007. As per the Energy Policy Act of 2005, MARS supports this change in 5.2.4.
- **Enhanced Raw Message Size Support.** Raw messages up to a variable size of 1.5 MB can now be stored.
- **Enhanced Raw Message Retrieval.** A new background process, keywordQuerySrv, runs in the background to index and process raw message queries. This process improves the response time. In additon, the display has been enhanced to display large events in a secondary window.
- **IP Log and Trigger Packet Enhancement.** Complete IPS events are stored in native XML format. A version field appears in the Packet data event header. IP logs are stored as base64-encoded text. Trigger packet data events (event type 6) and context data events (event type 7) are no longer created for new IDS/IPS events. Instead, they appear as links within the corresponding IDS/IPS event.

Note Keyword searches for strings will not match the IDS/IPS events unless those search strings are formatted as XML

- **New CLI Commands.** The show healthinfo and show inventory commands are exclusive to the second generation hardware.
- **Updated CLI Commands.** The following commands have been updated for the second generation hardware: raidstatus, hotswap, pnstatus, and pnrestore. In addition, pnrestore now supports restoring data in time slices.
- **Bug fixes.** For the list of resolved issues, see Resolved Caveats - Release 5.2.4, page 13.

New Vendor Signatures

The 5.2.4 release supports the same signature set as the 4.2.4 release. For details on that support, refer to the corresponding release notes as identified in Product Documentation, page 20.

Important Notes

The following notes apply to the MARS 5.2.4 and later releases:

- To enable monitoring support of Cisco Secure ACS, you must use pnLog Agent version 1.1 or later. Earlier versions of pnLog Agent will not work with the MARS 5.2.4 and later releases.
- Interfaces ethernet3 and ethernet4 are always down.
- USB keyboard does not work while re-imaging with DVD. Use the PS/2 port for keyboard support.

The following notes apply to the MARS 4.x and later releases:

- The performance of the Summary Page degrades when too many reports are added under My Reports. The smaller the number of reports under My Reports, the faster the Summary page loads. To ensure adequate performance, limit the number of reports to 6. This issue is partially described in CSCse18865.
- Do not to use DISTINCT or SAME in queries, and do not run multi-line queries. If you run such a query, the system time outs after 20 minutes without returning any results. The message “Timeout Occurred” appears instead. You can use DISTINCT and SAME in a Query to create a rule with the Query interface.
- For Symantec AntiVirus, the Symantec agent hostname (AV client computer name) appears in the “Reported User” column of the event data. Therefore, you can define a query, report or rule related to this agent based on the “Reported User” value.
- The False Positive and Query pages (multi-column result format) have changed. You can now query on firing events that triggered false positives within a time interval. Such queries will render events that did not appear on the False Positive page. To ensure performance, the False Positive page only displays false positives from the most recent 10,000 firing events. To view additional false positives, you must perform a query.

The following notes describe new behavior based on the resolution of specific caveats. Be sure to check the upgrade notes for each release for important notes on data migration.

Reference Number	Description
CSCsc50636, CSCsc50652	*Issues*: Backend IPS process runs at 99% CPU when pulling large IP Logs The backend IPS process reaches 1GB in memory used when pulling IP Logs. The process names depending on the version on MARS that is running: • In version 4.2.1 and earlier, the process names are pnids50_srv and pnids40_srv. • In version 4.2.2 and later, the process is named csips. These related issues, are specific to pulling IP logs from Cisco IDS/ IPS devices. The symptom is that the backend IPS service consumes the system resources on the MARS Appliance. As an improper configuration of the sensor can significantly degrade the sensor performance as well as that of MARS. *Workaround*: Ensure that settings for IP log creation on the sensor limit the size of the IP log (in terms of number of bytes or number of packets captured). Also, verify that IP packet logging is enabled only for signatures of interest and not for all signatures. In addition, the following release-specific maximums are enforced: • In 4.2.1, a 100 file maximum is enforced for the log file queue when the MARS is configured to pull IP log files. Therefore, it may not pull every IP log file. In addition, the complete IP Log file may not be pulled, instead, data is pulled from the file starting 5 minutes before the alert was generated through the end of the file. • In 4.2.2, a 1,000 file maximum (up from 100 in 4.2.1) is enforced for the log file queue when the MARS is configured to pull IP log files. The complete IP Log file may not be pulled, instead, data is pulled from the file starting 1 minute (down from 5 minutes in 4.2.1) before the alert was generated through the end of the file. And last, 100KB is the maximum IP log size that can be pulled from a MARS Appliance.
CSCsb71309	*Issue*: In MARS release 3.4.4 and earlier, queries that are run from a Global Controller that has no results returned from any of the attached Local Controllers will show up as “In Progress” in the GUI. This occurs in a Global Controller/Local Controller environment, and only when a global query returns 0 results from every one of the Local Controllers. *Workaround*: You may have to wait up to 10 minutes for a GC Query status to be marked as “Finished”, after all Local Controllers have finished running the query.
CSCpn02175	*Issue*: Data computed or stored on a standalone MARS while in standalone mode will not be transferred to a Global Controller. Only data computed on an Local Controller that is currently monitored by a Global Controller will be pushed up.
CSCpn02073	*Issue*: After renaming a cloud, clicking the cloud again causes an error. *Workaround*: Refresh the page before clicking a renamed cloud.

Reference Number	Description
CSCpn01270	*Issue*: The free-form search may not work for the following devices: • Check Point Opsec NG FP3 • Cisco CSA, 4.0 • Cisco, IDS, 3.1 and 4.0 • ISS, RealSecure, 6.5 and 7.0 • Entercept Entercept, 2.5 and 4.0 • IntruVert IntruShield, 1.5
CSCpn00247	*Issue*: The automatic time-out feature built into the GUI does not work when the Summary page is left open with automatic refresh selected. *Resolution*: Please log out of the system when you are no longer using it.

Caveats

This section describes the open and resolved caveats with respect to this release.

- Open Caveats - Release 5.2.4, page 5
- Resolved Caveats - Release 5.2.4, page 13
- Resolved Caveats - Releases Prior to 5.2.4, page 20

For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

Note If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

http://www.cisco.com/support/bugtools

To become a registered cisco.com user, go to the following website:

http://tools.cisco.com/RPF/register/register.do

Open Caveats - Release 5.2.4

The following caveats affect this release and are part of supported devices or compatible products:

Reference Number	Description
CSCsf31561	FWSM 3.1 syslogs FWSM-3-717001 till FWSM-4-717031 have missing colon
CSCsg00377	show resource usage command reports incorrect connection usage
CSCsg35110	MARS Global Controller cannot import a Local Controller SSL security certificate if the LC zone name contains a forward slash character (/)
CSCsf31401	MARS query does not highlight rules inside any policy group named Local

The following caveats affect this release and are part of MARS.

Reference Number	Description
CSCsi96790	Shared buffer gets stuck when near maximum size
CSCsi95074	low-traffic bytes ranking report causes process_inlinerep_srv to restart
CSCsi93594	Pnparser stops processing each time it tries to load the topology
CSCsi84817	MARS 4.2.5 - not categorising Windows Security event ID 672 properly
CSCsi71511	http status 500 appears while clicking the incident on the summary page
CSCsi64605	pnparser restarts frequently with sessionization turned on (default)
CSCsi60547	Long LC/GC disconnect leads to report sync problem
CSCsi52622	postfire lags behind due to doing large amount of NetBios name updating
CSCsi41173	If error occurs sending config change to LC, no other config sent
CSCsi39264	Cannot Configure an IDSM Module to PULL IPS logs
CSCsi32777	Configuring many events in drop rule can cause pink box error
CSCsi31867	csips crashes due to memory corruption
CSCsi29398	CS-Mars does mitigate to the proper endpoint
CSCsi28286	GC-LC upgrade to 4.2.4 resulted in Standalone display on LC
CSCsi23209	Some unsupported nfs cause system errors on MARS.
CSCsi19227	Some reports/rules/queries match events outside specified IP ranges
CSCsi18757	CS-MARS - Request to have the "ssldump" command in the MARS CLI.
CSCsi17607	GC - Zone Model for Auriga 210 showing as 200
CSCsi15769	NLS_LANG variable should be updated in environment
CSCsi15258	Accepting the collector, and source ip address as MARS ip address
CSCsi11963	MARS 4.2.4 not parsing IOS Router NAT properly
CSCsi09318	Mars - Using IE7, any query over 2 mins to process result in error
CSCsi08897	CS-MARS - CLI may display incorrect timezone after 03/11/07 DST change.
CSCsi04306	need to add CPU check for csips, csiosips, and cswin
CSCsi03686	CS-MARS - HTML/XML tags are not escaped when displaying packet context
CSCsi03658	CS-MARS - IOS Discovery via Telnet/SSH fails with $hostname in banner
CSCsi00963	CS-MARS Archiving Causes pidof[xxxxx] Messages to Appear on Monitor
CSCsh99201	MARS-Scheduled ranking report with ACTION filter produces empty results

Reference Number	Description
CSCsh97060	MARs says it can delete up to 500 at a time but only lets you delete 50.
CSCsh94361	Events with port 0 cannot be filtered using port in query/reports/rules
CSCsh93759	Rules/reports with large queries not working
CSCsh89885	Mitigation command not display properly in 4.2.4
CSCsh89445	GUI allow users create rule without putting rule name
CSCsh88897	race condition in pnparser triage handling caused syslog processing stop
CSCsh83068	Report and query return no results under device type ANY
CSCsh82939	MARS failed to restart if the hostname is changed after a restore
CSCsh77508	MARS is not displaying CSM icon for access-list syslog with severity 0
CSCsh75216	InLine multiColumn query case attachment Fails
CSCsh73553	USB Keyboard does not work while re-imaging with DVD
CSCsh71162	Doc enhancement Mars GC push down IP Mgr group to active LCs
CSCsh69765	CLI date/time/ntp commands should reboot if time change exceeds 30 mins
CSCsh68503	ISS SNMP trap: need to parse another format for ICMP type/code fields
CSCsh64155	MARS is not sending all the parameters to CSM for ASA acl syslog
CSCsh58754	4.2.2->4.2.3 upgrade sometimes stalls, succeeds after repeated tries
CSCsh57236	Unknown Reporting Device was missing on GC's DB pn_device table
CSCsh56931	Rule engine fires only once if only SAME is present in any column
CSCsh52537	Repeated upgrades 4.2.2->4.2.3 fills hard drive
CSCsh51271	GC is unable to update LC's device name under admin/LC management
CSCsh47461	'Details' button does not return
CSCsh44179	Connection Errors cause inability to select zone in incident/rule edit
CSCsh42151	GUI Summary pg shows #events < #sessions & negative data reduction rate
CSCsh39200	MARS charts only display the data for few days
CSCsh38818	GC-LC upgrade 4.2.2->4.2.3 results in inverted online-offline status
CSCsh36853	overflow condition in FileSystemFull function (pnbfs.cpp)
CSCsh35953	MARS unable to add similar named contexts from different fwsm
CSCsh29243	MARS Device Type label needs to reflect support for IOS 12.2 and later
CSCsh22871	User can create a device named ANY
CSCsh20219	Confirmed user false positive query error java.lang.NullPointerException
CSCsh18265	null drop rule causes parse error in the GUI
CSCsh14454	server.log can grow unbounded with in a single day
CSCsg98026	pnlogagent causes acs log files to add (01) to file name
CSCsg91816	Query for ICMP port 0 shows UDP/TCP results
CSCsg86481	CS-MARS parsing error for ASA7.0 msg 302018
CSCsg83055	parsing error for FWSM-n-302003 and FWSM-n-302004
CSCsg80475	All incidents purged if event-session partition table is corrupted.

Reference Number	Description
CSCsg79246	Getting a blank window when adding a device in IE 7
CSCsg76958	FR: Recognize either CIPS network variables or have CSMARS net variables
CSCsg75303	GC: If chose LC specific device in rule, it doesn't pass to LC correctly
CSCsg74922	MARS: License invalid after re-image from 3.4.3 to 4.2.2
CSCsg73843	GC - Unable to change configuration information (email IP) from GUI
CSCsg73786	Devices should not be added to MARS if Discovery is unsuccessful
CSCsg70386	SSL uses key less than 1024
CSCsg69859	SNMP Layer 2 Discovery Error, when community string has been corrected.
CSCsg66801	Activity: All Events and NetFlow report chart is missing on summary page
CSCsg64986	Custom column query - got pink box if chose a rule as a filter
CSCsg64951	Certain ASA 7.0 syslogs do not get parsed by MARS
CSCsg64704	DNS wasn't configured correctly,Pausing event processing for 40 seconds
CSCsg60114	System error when generating NAC report
CSCsg54313	ORA-01654: unable to extend index on MARS 200
CSCsg53084	MARS - WebVPN ACL Parse error event fires on incorrect syslog
CSCsg49227	Mars - Events from multiple ids sources are incorrectly sessionized
CSCsg47022	CS-MARS - Incorrect Start Times on Retrieved Raw Message Files
CSCsg44725	need to downgrade log level of CSA snmp trap errors in backend log
CSCsg41549	MARS discovery issues with Loopback IP on IP Unnumbered interfaces.
CSCsg41027	MARS - Retrieve Raw Messages Fails at 0%
CSCsg38029	high CPU usage in pnparser due to checkpoint NAT rules
CSCsg26352	Getting a internal server error when trying to access a incident on GC
CSCsg26225	Graphs/Images do not show up in case related report emails
CSCsg20987	CSMARS DTM sdf files are sent with invalid format
CSCsg20514	Mars backend processes need to save backtraces on a crash for debugging
CSCsg20408	FW-6-SESS_AUDIT_TRAIL Parsing Error
CSCsg16843	MARS reporting misleading licensing problem while trying to add a LC.
CSCsg14082	Default query Changed in system defined report
CSCsg13767	SuperV doesn't detect/restart processes
CSCsg10787	CatOS telnet discovery failing.
CSCsg08166	Unable to discover ASA 7.0 Error:There is no Error Log for this Device
CSCsg06339	Getting a Timeout Occurred error when running a query with != as service
CSCsg04079	Lotus Notes client gets JavaScript error with emailed MARS report
CSCsg02749	custom column report generates empty results
CSCsf99844	wrong values for current connections using CLI "show resource usage
CSCsf96634	MARS cannot discover new route added to a router
CSCsf31228	Unknown device events for FWSM 3.1 FWSM-3-717001 till FWSM-4-717031

Reference Number	Description
CSCsf31207	Mars doesn't support new/changed FWSM 3.1.3 maintenance release syslogs
CSCsf31121	Exception in Case Management code when deleting a report
CSCsf30116	Event Rate on the Top Destination Port graph is not correct
CSCsf26715	Inaccuracy in per-context memory utilization for multi-context devices
CSCsf18192	Slow rendering of the GC/LC Summary page
CSCsf12825	GUI should prevent edit/delete of system-context PIX/ASA 7.0 devices
CSCsf11651	Device resource monitor incorrectly samples 5 sec CPU instead of 5 min
CSCsf06819	vulnerabilities not updated for hosts reported by deleted eEye console
CSCsf06141	high CPU usage in pnparser sessionization
CSCsf06019	Generic Router UI must support multiple reporting applications
CSCse99039	Redundant tab add available module under Device type Cisco IOS 12.2
CSCse98046	need to improve db partition rotation strategy
CSCse98029	Occasionally corrupted event data enters into MARS database
CSCse91636	MARS - not all columns seen in CSV reports generated using custom column
CSCse88764	can't access a ftp server with a user ID/password including @
CSCse85564	Cannot add devices to a report which has more than 35 devices.
CSCse84962	eEye: MARS does not remove resolved vulnerabilities from host info
CSCse82042	Change the Device Type Version for FWSM
CSCse82022	Unable to view reports starting with #sign in csv format
CSCse82017	View HTML option for reports turns back to default report format - csv
CSCse78738	FWSM ifspeed incorrectly reported as 0 for per-context vlan interfaces
CSCse78089	Unable to upgrade CS-Mars via GUI
CSCse73788	MARS rediscovers Juniper Netscreen firewalls with wrong OS
CSCse60240	CS-Mars - report for old events include real-time events
CSCse56632	Browser hangs if a device is added with more than 50 monitored networks
CSCse54976	Some incidents are not written to DB
CSCse54808	The time stamp shown by the pndbusage command is incorrect.
CSCse52782	Can't change run-time to day in "Resource Issues: Server - Top Reporting
CSCse52217	Customer gets pink box in GenericHostDeviceEditManagement.jsp
CSCse45884	LLV query causes client CPU to go to 100%
CSCse45018	MARS is unable to parse NetScreen 5.x syslogs
CSCse42953	CS-Mars - unable to show L2 path when source and destination in same net
CSCse39426	frequent superV & pnparser restarts cause log processing to fail
CSCse38565	CSV-Re-importing Symantec AV client CSV doesn't work
CSCse38356	Windows pulling gets stuck for one IP due to invalid content in evt log
CSCse35758	Inability to trace when first and last event occurred on a query
CSCse35420	Interface error rate should be separate from discards and unknown protos

Reference Number	Description
CSCse34600	configurable SNMP timeout support
CSCse34407	Query Tab -> Multi column query returns wrong results.
CSCse33688	No Event Types listed under Cisco Switch-IOS 12.2
CSCse33172	Invalid id used in DbClient::retrieve() 0
CSCse32591	dealing with duplicate hostnames in VA import
CSCse31722	Cloud toggle only works on first page of reporting devices
CSCse27948	pink box when do query - ORA-01555: snapshot too old exception
CSCse26964	CatOS Syslog %SYS-4-P2_WARN not parsed correctly by MARS
CSCse23191	Disable 'No Pager' cmd sent by MARS to PIX, ASA, FWSM firewalls
CSCse23176	MARS Global Controller not producing alerts when losing LC communication
CSCse23051	viewing report of query type of MAC addresses report got pink box
CSCse22838	can't find priority for CSA NT-Event-Log events
CSCse21626	Clicking activate is not taking effect
CSCse20593	CSM device type could not be added one time (OK most times)
CSCse19198	Device Cnf: Changes in Mail Gateway IP doesn't reflect Report/ Notif
CSCse18816	UI takes 99% CPU, hanging browser and slowing system while expanding all
CSCse18240	DOC: cs-mars doesn't handle vpn paths
CSCse17936	5K Lines Custom Query fails
CSCse13038	CS-Mars - learning of McAfee agents with invalid names
CSCse11258	After group is deleted, items under "All" group not shown
CSCse10945	Summary Page Graphs Spontaneously Change Displayed Size (w/ multi-head)
CSCse09127	Failed load from csv returns incorrect status
CSCse07425	JVM is using up to 1.5 GB on a GC or LC
CSCse03237	Changes made to GC network groups are not propagated to active LC rules
CSCse03134	More control is needed over retrieve raw messages and cleanup
CSCse03097	CheckPoint LEA record comes to MARS later and later
CSCse00668	rule definition changes can lead to empty reports
CSCse00626	IP Management -> device group displays hosts only.
CSCsd95582	Both successful/failed mitigation reports show same results
CSCsd93480	FOLLOWED-BY in rules has looser constraints than sometimes desirable
CSCsd92916	CS MARS - Raw Ip Addresses in Custom Query email have incomplete URL
CSCsd92285	Security Dev Edit page does not check for existing IP address conflict
CSCsd90181	increasing pnrestore robustness
CSCsd89457	Incorrect handling of time range for rules that fire periodically.
CSCsd86896	Clicking the clear button when editing the query type doesn't work.
CSCsd84350	CS-MARS/CSM: Credentials change on CSM side not checked.
CSCsd74283	changing report-result retention limit

Reference Number	Description
CSCsd73486	Mars: Not able to recognize the event type for ISAKMP and IPSec messages
CSCsd69137	Default Group in Scheduler need to be made to Run On Demand
CSCsd69063	Reported User with single-quote (') causes oracle error
CSCsd61749	pnrestore doesn't restore all of the system config
CSCsd53173	Retrieve raw messages doesn't properly update the progress percentage
CSCsd48544	port 8444 required for GC/LC communication
CSCsd48097	Event processing may stop if pnparser creates shared buffers first
CSCsd37005	user must be able to change own password
CSCsd28590	CS-MARS - Inactive Reporting Device Rule is not configurable
CSCsd22832	Attempt to remove IP subnet from IP Management fails, with error
CSCsd20196	User and System Scheduled Reports fail to display data
CSCsd15695	Summary dashboard showing incorrect statistics for false positives
CSCsd13969	resetting italics for GUI links
CSCsd06302	device name with single quote causes pink box
CSCsc97963	Netscreen logical interfaces (vlan intf) not discovered
CSCsc95831	log messages of MARS processes stopped being written into backend log
CSCsc91572	Multiple target ports in IDS event show up as 'port 0' in query
CSCsc90480	MARS Incident notification options are not configurable
CSCsc87501	if set IP address to 0.0.0.0 box trying to reboot
CSCsc78878	snort signature 2570 incorrectly mapped
CSCsc73832	Drop rule inactive for events received by netflow in CS-MARS
CSCsc59363	Need improvement to GUI for multi-line rules
CSCsc58485	5 tuple information missing from downloaded raw log file
CSCsc48498	CS-MARS: Upgrade from 3.4.x fails
CSCsc42396	CS-MARS Viewing IP of grouped sessions throws Exception, no Time var
CSCsc30107	Cs-Mars - Queries with != in service column don't work
CSCsc15590	MARS not including all events in a report, query returns events fine
CSCsc04484	LC Rule/Report list shows empty after deletion of GC group
CSCsb80082	Deleting a LC w/o exchanging certificates doesn't set mode to Standalone
CSCsb77550	CSV-re import of CSA and Symantec agents unsuccessful
CSCsb67871	Got System Error In GC After Re-installed New Version In LC
CSCpn03077	GC, sys error when adding a LC which was added to GC already
CSCpn03057	Copied rules have shortened year in front, which is confusing (ex. 0
CSCpn03052	JBoss 'OutOfMemoryError ' when accessing Management/Event Management
CSCpn03005	Loading Resource Util report as On-Demand query produces a system error
CSCpn02976	GC:LC - Communication issues after time zone change
CSCpn02973	Not able to downgrade a security analyst to Notification only user

Reference Number	Description
CSCpn02968	Network group search is not working for "All IP addresses
CSCpn02901	GC/LC, rule does not display user <cxu> but allows such cfg
CSCpn02883	Event management search works only for event description
CSCpn02869	Rules editing: changing entry for select window pulldown after error
CSCpn02804	Replay History feature not working correctly
CSCpn02688	GC/LC: gc lc displayed diff time rage for the same global report
CSCpn02666	Batch Query Results with one item returned -> no data in graph in em
CSCpn02656	System error occurs when # of java connections runs out
CSCpn02653	No way to specify "!Keyword" without a good "keyword
CSCpn02594	LC: Path/Mitigate link throws up a pink box after the device has bee
CSCpn02574	Time change on system causes GC/LC communication problem
CSCpn02566	rebooting mars while it is upgrading cause the box not accessible
CSCpn02558	"Agent" didn't be removed correctly
CSCpn02549	JavaScript Error from ViewReport when clicking Edit/Clear
CSCpn02511	need to fix errors in affected os
CSCpn02470	Server csv function could not handle special characters in password
CSCpn02414	GC/LC user rule is too long to fit into a page if keyword is long
CSCpn02410	rule was not fired because Oracle log used upper case for user
CSCpn02398	XML escaping errors in Keyword Search in Rule
CSCpn02385	Applied $TARGET01 for GC Query Source IP resulted in "resultCounter
CSCpn02383	IIS parsing must be separated from Windows log
CSCpn02251	License: Upon entry of 100 license onto 100e, need to restart pnpars
CSCpn02177	Docs: Filesystem Check after 22 reboots
CSCpn02061	Saving .csv files under WinXP SP2 results in .htm extension
CSCpn02011	discovery for special passwd 1"1 failed
CSCpn01489	BQ: Query summary doesn't mention "severity" if it's a criterion
CSCpn01438	Batch Query: Under high load, some batch queries may not complete
CSCpn01416	Select: Temp paging fix on Notification-SNMP page
CSCpn01398	Unable to shutdown an interface
CSCpn01382	Security device type hosts don't show up in IP management
CSCpn01319	pnreset command does not cause reboot
CSCpn01293	Host OS listing needs cleaning
CSCpn01219	Cleanup script for invalid /etc/qpage.conf entries
CSCpn01134	Cloud name input box accepts invalid characters
CSCpn01051	Browser: Open non-supported browser to MARS causes other browsers to
CSCpn01045	Archiving: Need better error message
CSCpn00908	"Domain" in Configuration page - no use

Reference Number	Description
CSCpn00610	Backend logs can be out of order in the view page
CSCpn00596	RelNote: Events and Sessions counts can be out of synch
CSCpn00586	nasl message text needs to be changed
CSCpn00455	Graph doesn't refresh when a cloud is renamed
CSCpn00293	using TAB in editing fields
CSCpn00259	Setting Logging Level for "GUI" to "Trace" and saving -> "Debug
CSCpn00212	Graphgen crashes when there are many non-existent devices
CSCpn00183	Adding devices w/o "Activate" can cause "messy" graph
CSCpn00173	Nessus should check pre-NAT address instead of Post-NAT address
CSCpn00166	Inconsistent behavior for "ANY" in Rules and Queries
CSCpn00146	Report names that differ by only slashes or dashes conflict

Resolved Caveats - Release 5.2.4

The following customer found or previously release noted caveats have been resolved in this release.

Reference Number	Description
CSCsi17782	Some OS/application setting not archived.
CSCsi14821	Raid build process improvement to disable rebuild in pnmonitor
CSCsi14133	Oracle process listening on TCP port 32771
CSCsi08897	CS-MARS - CLI may display incorrect timezone after 03/11/07 DST change.
CSCsi07845	RAID Email Message contains invalid Model and disk size
CSCsi07837	Raid Notification Email contains an outdated email address for sender
CSCsi07329	no CLI message after executing hotswap add
CSCsi05707	JBOSS shut down in the middle of Raw Message Retrieval
CSCsi02709	Custom Parser: Patterns not displayed in the correct order
CSCsi02398	CmdTool2 generates unsolicited log MegaSAS.log
CSCsi01312	Guide should state what services needs to run on GC
CSCsh93152	pnrestore very slow restoring perf test (high volume) data
CSCsh91852	5.2.3: Need schema update to 5_2_39
CSCsh88897	race condition in pnparser triage handling caused syslog processing stop
CSCsh86017	Pink box in GC OutOfMemoryError
CSCsh85870	Admin->Maintenance->Retreive Raw Message causes out of memory error
CSCsh85331	LC installation on 110 does not complete - /etc/model not created
CSCsh84212	pnmonitor does not detect and rebuild failed HDD
CSCsh81862	Recovery DVD to restore OS to flash
CSCsh81848	Auriga-2 demo license has only one license file for all models

Reference Number	Description
CSCsh79934	ORA-01555 during GATHER_STATS_JOB encountered errors
CSCsh78439	Gc to LC: edited user rule not in rule group when passed to LC
CSCsh78162	include debug tools in Auriga-2 deployment
CSCsh73187	DB filling up during purge test due to mis-sizing in MARS 110
CSCsh73053	TopN Bar and Pie Charts fail to appear for queries
CSCsh72008	DELETING_LC_STATUS constant should keep the same value in all releases
CSCsh70637	'View Decode' is broken on doing a query with certain keywords
CSCsh68073	pnreset -s will not run
CSCsh67287	t_semaphore class not thread safe
CSCsh64940	Mismatch between IpLogIDs from raw_msg and keyword query
CSCsh64731	Add SN for HDD, BBU and Power supply in "show inventory
CSCsh63511	Extra analyzer related commands
CSCsh63214	RawmsgRetriever may Cannot retrieve Rawmsg for some events
CSCsh61683	Need to change pnsh code based on INTEL's new CmdTool2
CSCsh61278	Pink box while viewing IpLog data
CSCsh60413	LC pulls data very slow when encountering DbException
CSCsh60091	5.2.3 DVD installs on Gen1 hardware
CSCsh59843	Auriga: upgrade libesmtp version to match MARS 4.2.3
CSCsh57063	email was not sent out when sudden increase traffic rule fired
CSCsh56683	Scalability LC-GC sync gets stuck. LC has 100's thoursands of devices
CSCsh56499	Mars should learn FWSM dynamic nat from syslog for sessionization
CSCsh55827	pnrestore fails to restore Report result and statistics result in full.
CSCsh55679	TCP port 1098, 4445, 8083 are opened
CSCsh54369	Ranged restore failure
CSCsh54366	pnrestore can not import dynamic data
CSCsh54049	Custom column query: cache is not cleard from option page
CSCsh52585	license file name with space in between will cause remove and rename not
CSCsh52269	'Unknown Reporting Device' should not be pushed to GC
CSCsh52035	Entering expert mode does not require Cisco-part password
CSCsh51096	move /var/tmp from flash /
CSCsh49698	Make QueryRawMsg JNI call thread safe
CSCsh46868	Custom column query not returning data
CSCsh45686	wrong version of pnreset in 5.2.3 build - missing -s option
CSCsh45675	Pink box on GC device page
CSCsh45547	add check for "blank event type name" in datawork convert/check script
CSCsh45319	keyword search return incorrect result
CSCsh44319	correct wrong "Affected Platform" entries in 1c-bigFile

Reference Number	Description
CSCsh44210	pink box while doing CSM policy query
CSCsh43697	Must click "activate" on all LC's after creating a rule on a GC
CSCsh42365	DbClient default assignment operator memory leak
CSCsh40743	pink box when doing real time query and click access rule icon
CSCsh40298	Test Connectivity Fails with alternate Qualys Device IP address
CSCsh39917	VPN device discovery using incorrect SNMP string does not give error
CSCsh38718	Batch Query does not complete (remains "in progress")
CSCsh36648	archive/restore - pnrestore error restoring from local image (-m 5)
CSCsh35192	Need to update Oracle to 10.2.0.3
CSCsh35130	Cancel edit removes Enterasys/NS IDP Server and sensors from device list
CSCsh34493	ranged pnrestore starts restoring data w/o asking user's confirmation
CSCsh34067	ArchiveRestore / CLI Negative Test - inconsistent error messages
CSCsh32558	custom column query: for acs event log, reported user is missing
CSCsh31253	Rules can't be edited after upgrade from 4.1.5 to 4.2.3
CSCsh29599	pnrestore does not show proper error when stage dir does not exist
CSCsh29590	glibc detected *** malloc(): memory corruption
CSCsh27853	Report results for a 10 minute window is dropped on an 'activate
CSCsh25607	TopN Signature pulling is not working
CSCsh25594	GUI allows user to select HTTPS as archiving protocol
CSCsh22767	"Admin/Maintenance/Retrieve Raw Messages" need to be disk space aware
CSCsh22252	pn_device_et_stats mismatch before archive and after restore
CSCsh20653	GC2R shown as GC2 in show inventory command
CSCsh20617	Java error after trying to license GC2R system
CSCsh20219	Confirmed user false positive query error java.lang.NullPointerException
CSCsh19873	Auriga: Need to change sem_wait() code due to glibc pthread lib change
CSCsh19831	new rpcclient2 binary to be packaged with a fix for CSCsh18285
CSCsh19644	Get browser error when select to add a new host
CSCsh19573	Get License Error when login after timeout on page
CSCsh18265	null drop rule causes parse error in the GUI
CSCsh17705	ssh command for Mitigation uses wrong parameters
CSCsh15821	CLI command's hostname incorrectly changes the hostname to DbClean
CSCsh15700	Purging of temporary tables failing
CSCsh14842	MARS can't receive the scheduled reports from qualys guard
CSCsh14075	scheduler-service.xml.contrib present in deploy directory
CSCsh13246	Merge 4.2.3 data to Auriga
CSCsh13238	Change upgrade script to allow upgrade process complete
CSCsh13081	crontab jobs missing on Auriga install image

Reference Number	Description
CSCsh11546	pn_event_id needs to be updated during restoration
CSCsh11543	TEMP tablespace needs more space allocated in 110/210
CSCsh11027	clicking 'next' button for IOS hangs up on GC
CSCsh06662	Discovery broken and user not prompted when device is configured from GC
CSCsh06597	root dir is 100% and Oracle could not start after power outage
CSCsh04794	Data Issues on install/upgrade
CSCsh04784	java crashed when user run matching raw msg query
CSCsh04624	LC cannot be added to GC
CSCsh02908	The order of backend processes change randomly when setting log level
CSCsh02707	user can add IDS3.1 devices in Auriga
CSCsh01620	The javaDbTool did not handle NULL value dump correctly.
CSCsg99611	CS-MARS - Radio buttons are confusing on Retrieve Raw Messages page
CSCsg98984	DB Creation scripts being split up and need integration into the build
CSCsg98826	LC interfaces are missed in the All IP Address list on GC
CSCsg98822	A device on GC(pushed from LC) is not deleted even after deleting LC
CSCsg98574	pnsuperv not working properly
CSCsg98310	Discover failed for CheckPoint Opsec NG FP3 device
CSCsg98238	paging nitification does not work, modem is not working
CSCsg96935	the cmd 'show' is not sorted with the rest of CLI commands
CSCsg96931	sh inventory shows some un-related info for battery bkup
CSCsg96923	show healthinfo displays garbage characters
CSCsg96890	CLI hotswap takes ? as disk 0
CSCsg96883	CLI show inventory still shows the removed power supply
CSCsg96765	110R/GC are shown as 110/210 in show inventory
CSCsg95402	New reports for 4.2.3 spelled 'Certificates' incorrectly in report name
CSCsg95031	Cannot download raw message file from csmars
CSCsg95001	Qualys: Search on Internal Syslog Events does not return any results
CSCsg94901	LLV causes IE stuck when raw message is very long
CSCsg94880	GC Pink box when doing keyword search on GC
CSCsg93890	Auriga performance capacity is more than its rated limits
CSCsg93306	Hosts List on MARS not consistent with discovered Qualys device list
CSCsg91976	Need to update Cisco logo and copyright year
CSCsg91955	user not prompted when policy query icon is clicked first
CSCsg90400	can not retrieve raw message
CSCsg90388	Keyword not highlighted
CSCsg90367	/u01 partition is full
CSCsg88549	keyword query stuck inside oracle

Reference Number	Description
CSCsg86861	Only 4000 characters displayed for keyword search large raw messages
CSCsg86757	Using telnet discovery wrongly merged VLAN1 info into VLAN13 info.
CSCsg86433	device_monitor module restarts
CSCsg86170	pnarchive partition is full and pnarchiver is stuck at 99.9% cpu usage
CSCsg85296	GC: Upgrade - Syslog 100032 and 100044 are not sent.
CSCsg82796	/ could be full and causes pnupgrade fail
CSCsg82722	cannot change GUI runtime log level from debug to trace
CSCsg82666	PnUtils::sendPacket() does not close sockets in case of socket errors
CSCsg82353	User not prompted when there is a certificate change for CSM
CSCsg82231	Test Connectivity failed message for CSM results in Unknown Event
CSCsg82210	Video stopped working on GC 210 upon pwr off-> pwr on
CSCsg81200	some syslog messages are not generated for CSM
CSCsg81038	'New' should be removed from Event type name
CSCsg79166	UPGRADE: When certificate is rejected, error should be displayed.
CSCsg79071	Deleting an SSL device doesn't delete the certificate from MARS cache
CSCsg78885	After Rejecting Certificate for CSM Device , exception is thrown
CSCsg78512	Can't discover the device anymore when fingerprint is changed
CSCsg77562	syslog messages: %MARS-3-100041 is not generated
CSCsg77548	syslog messages: %MARS-3-100043 and %MARS-3-100 are not generated
CSCsg77522	SSL and SSH generates syslog messages differently on discovery
CSCsg76940	Adding Switch-CatOS ANY device shows pink box error
CSCsg76793	Suspended LC still communicates with GC
CSCsg75149	LC Upgrade from GC : Inconsistent certificate validation.
CSCsg73962	Serial Connection Baud Rate Fixed at 19200 instead of 9600
CSCsg73604	5000Line_InlineQueryAsBatchEventSession5KPlus
CSCsg73590	Changing status of user confirmed positive type incident yeilds pink box
CSCsg72246	auriga-2: intruvert not parsing event correctly
CSCsg71475	Submitting Unconf. FP Firing Event only query generates system error.
CSCsg71446	device_monitor module restarts every 3 to 5 minutes
CSCsg69917	auriga-2: queries by keyword not work consistently
CSCsg69279	Bad View Error data if user closes prompt window for fingerprint/cert
CSCsg68371	cannot not use < > & to do keyword correctly
CSCsg67502	Incident->False Positive note is grammatically incorrect
CSCsg66896	Dynamic restore doesn't work
CSCsg66569	110E / 110R
CSCsg66099	Devices from deleted LC should be removed from the GC
CSCsg65219	5K line InlineQueryAsBatchMultiColumn5K/5Kplus/Non5k cases fail

Reference Number	Description
CSCsg64487	Popup Window is blank when adding intruvert manager
CSCsg64377	raw_msg for IPS/IDS alerts doesn't display in HTML with keyword search
CSCsg64135	5000Line_InlineQueryAsBatchEventSessionNon5K returns <or> than defined
CSCsg63105	raw messages for IP logs are not displayed correctly
CSCsg62983	GC Topology doesn't merge - janus.conf file has mergeTopoTimer=0
CSCsg62921	License Agreement page is displayed even if license is invalid
CSCsg62852	5000Line_InlineQueryMultiColumn5K doesn't complete;gives a system error
CSCsg62192	Netflow Config Info is not saved
CSCsg61262	no page title for adding intruvert sensor
CSCsg61162	csips and csiosips restarts on clicking 'Activate'.
CSCsg61041	query for a raw message sometimes displays raw message can't be retrieve
CSCsg60756	some signatures are missing from virtualsensor.xml file
CSCsg60652	Vulnerability Scanning Network Definition is not saved
CSCsg60565	All keyword queries failed
CSCsg59821	subscription files are not created under /tmp/iosips and /tmp/ips
CSCsg59213	License server needs to be udpated with latest CSMARS models
CSCsg59157	Blank screen while adding CSA console w/Enterasys Dragon Sensor as agent
CSCsg58962	Auriga: Serial Connection not available for direct access to box
CSCsg58867	Zombie process is detected but not be killed
CSCsg58797	pnarchiver fails - won't stay up
CSCsg58448	CLI telnet command does not work
CSCsg58446	CLI tcpdump command does not work
CSCsg58021	raw message data is kept in two places while archiving is *not* enabled
CSCsg57593	CLI's domainname accepts single word domain name
CSCsg57535	CLI's domainname accept invalid characters
CSCsg57440	CLI dns incorrectly display ipaddress
CSCsg57403	Auriga: Expert password needs to be reset to expected password
CSCsg57249	CLI Date command fails to set system date
CSCsg57182	GUI uses backend instead of jni call to retrieve raw messages
CSCsg56525	Keyword search: wildcard * failed
CSCsg56470	SNMP Notification is not sent when rule is fired
CSCsg56320	Hotswap commands not available on GC and LC
CSCsg54634	NetFlow valid networks gone after submit
CSCsg54328	pnparser process stops during performance testing
CSCsg54313	ORA-01654: unable to extend index on MARS 200
CSCsg54045	System Notification does not send out email when HD Failture
CSCsg53796	System Analyst can create a Admin account.

Reference Number	Description
CSCsg50832	ntp command doesn't work
CSCsg50811	DTM Notification allows user to add without recipient
CSCsg50676	Deleting a Service/User Management Group forwards to empty page
CSCsg50590	XML Notification does not work
CSCsg49598	Admin / Retrieve Rawmsgs: get raw message semaphore error
CSCsg49273	Select All doesn't work when user is already selected.
CSCsg49198	can't add on-demand or on-schedule discover
CSCsg48971	Auriga GC restarts frenquently
CSCsg48020	GUI, GC displays eth0/eth1 info in a way different from 4.2.2
CSCsg47494	rpcclient2 for windows pulling missing
CSCsg46621	Incident query ranked by time: wrong logic
CSCsg46204	Can't add IP Management Group
CSCsg45955	cannot add valid network
CSCsg45933	sslcert doesn't work
CSCsg44820	FelxLM license uploading failed
CSCsg44814	failed to start Oracle after DVD installation
CSCsg44797	Sanity Test-discovered system issues
CSCsg44319	JDK DST handling problem requires JDK update
CSCsg43508	pink box for Admin->System Maintenance->Retrieve Raw Messages
CSCsg43367	CLI ? and help not working in Auriga 210 model
CSCsg42931	Inconsistant search box behavior.
CSCsg42907	pink box: /Admin/Retriever/GetRawMessages.jsp
CSCsg42639	Single quote in variables or host name text box causes browser to hang
CSCsg41130	Include the libcurl.so for 4.2.3 and 5.2.3 release
CSCsg37886	error log exception when user_id is 201 (with Case Management)
CSCsg26349	UI doesn't display XML raw message with XML tags
CSCsg25261	Backend crash and restart need to clear RawmsgRetrievalCache semaphore
CSCsg02749	custom column report generates empty results
CSCsg00370	Suspending a LC in deleting cause abnormal state transition
CSCsf95930	Need to check certs presented by devices and drop conn if cert changes
CSCsf32615	Archiving can fill the / partition, disabling the Mars
CSCsf30059	Wrong version of pnmonitor installed on MARS 110
CSCsf27617	pnparser enhancement - custom parser to expand three more user fields
CSCsf20103	csips and csiosips occasionally crashing
CSCsf11055	CC: GUI and CLI allow different password lengths - should be same
CSCse98046	need to improve db partition rotation strategy
CSCse98039	pnarchiver on new platform is consuming 100% cpu

Reference Number	Description
CSCse95030	device_monitor memory leaking when reading /snmp/data
CSCse89531	4.3 merge: LLV is not functional
CSCse73868	pnrestore command should support end-time argument in the command line
CSCse68056	Can't chage the GUI logging Level to trace
CSCse53870	Change Protego OS string to reflect Cisco
CSCse38615	Bucket_size field in pn_report_result table is negative
CSCse34135	domainname did not filter invalid domainname input
CSCse34123	Incmprehensible error message for CLI
CSCse29860	UTC and GMT time zone missing
CSCse27948	pink box when do query - ORA-01555: snapshot too old exception
CSCse27493	Cisco IDS raw messages in CS-MARS should contain the 5-tuple
CSCse22824	CS-Mars - device_monitor: change resource not found log level to debug
CSCse21936	Daylight savings time affects the custom parser's received time field
CSCsd62041	PnLogger causes process crash
CSCsd57224	pnstatus results in different statuses for modules evrytime it is run
CSCsd25868	CS-MARS Inactivity report is not updated in netflow processing
CSCsd23663	Query for raw_msg field always results in zero
CSCsc47210	inline process srv could crash
CSCsc20710	IP Log & Trigger packet data from MARS UI can't be converted into pcap
CSCsc07684	FR: CS-Mars no requirement for service provider for user creation
CSCsb18609	OS 4.0: pnparser re-arrange the way to use seteuid
CSCsb18604	OS 4.0: Failed to discover CheckPoint device
CSCsb14422	OS 4.0: Pnesloader was towed down when pnarchiver went dead
CSCsb12674	OS 4.0: jboss script warning message
CSCpn03005	Loading Resource Util report as On-Demand query produces a system error
CSCpn02693	6MB mem leak in process_event_srv after each activate

Resolved Caveats - Releases Prior to 5.2.4

For the list of caveats resolved in releases prior to this one, see the following documents:

http://www.cisco.com/en/US/products/ps6241/prod_release_notes_list.html

Product Documentation

For the complete list of documents supporting this release, see the release-specific document roadmap:

- *Cisco Secure MARS Documentation Guide and Warranty*

  http://www.cisco.com/en/US/products/ps6241/products_documentation_roadmaps_list.html

Lists document set that supports the MARS release and summarizes contents of each document.

For general product information, see:

http://www.cisco.com/go/mars

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, 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