Release Notes for Cisco Security MARS Appliance 5.2.7

Revised: October 25, 2007, OL-14222-01

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 5.2.7 running on any Local Controller or on any Global Controller. They provide the following information:

Introduction

Version 5.2.7 is now available as an upgrade of 5.2.4 of your 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 5.2.7 from the Cisco support website at:

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

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

Supported Hardware

Cisco Security MARS Version 5.2.7 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 2

Miscellaneous Changes and Enhancements

The following changes and enhancements exist in 5.2.7:

- **Oracle 10g Support.** Previously, MARS supported only Oracle 9i. Support for 10g has been added.
- **Snort 2.6 Support.** Previously, MARS supported only Snort 2.0. Support has been added for versions up to and including 2.6; however, all versions of Snort are selected from using the same Snort 2.0 value in the drop down list when adding a software application to a host under Security and Monitoring Devices. No new options were defined.
- **Update to 3rd-party vulnerability assessment signature sets.** This release includes many new vendor signatures, updating the 3rd-party signature support. For more information on the updates, see New Vendor Signatures, page 2
- **Bug fixes.** For the list of resolved issues, see Resolved Caveats - Release 5.2.7, page 15.

New Vendor Signatures

The following table describes the most recent signatures supported for each product or technology:

Revised in 5.2.7	Product	Signature Version Supported
Yes	Cisco IDS 4.0, Cisco IPS 5.x, Cisco IOS 12.2	Current through S291 signature release.
Yes	McAfee Entercept HIDS 6.x	Current through the June 11, 2007 signature release.
Yes	ISS RealSecure Network Sensor 6.5 and 7.0, and ISS RealSecure Server Sensor 6.5 and 7.0	XPU 27.010 Release date: May 8, 2007
Yes	McAfee IntruShield NIDS 1.8 McAfee Network Intruvert v 2.1.9.104	2.1.68.5 Release date: June 12, 2007
Yes	Snort NIDS 2.6.1	Current through the May 14, 2007 signature release
No	Netscreen IDP 2.1	Signature version: 2.1 r7. Release date: March 10, 2007
Yes	Enterasys Dragon 6.x, 7.x	Current through the June 9, 2007 signature release.
No. EOS.	Symantec Manhunt 3.x (See Symantec NIDS, v 4.0.)	3.4.3 Update 59 Current through the May 24, 2007 signature release.
Yes	Symantec NIDS, v 4.0	Signature package: 80, 81 Release date: May 9, 2007, May 24, 2007 respectively
Yes	Qualys QualysGuard 3.x, 4.7.161-1	Current through the June 10, 2007 signature release.
Yes	E-Eye, Retina Scanner Vulnerability Software, version 5.6[1]	Current through the June 11, 2007 signature release.
Yes	Foundstone, version 4.x	Current through the June 14, 2007 signature release.
Yes	CheckPoint Application Intelligence (VPN-1 NG with Application Intelligence R55)	Current through the April 26, 2007 signature release
Yes	Common Vulnerabilities and Exposures (CVE) Database	Current with the May 10, 2007 definition update.

1. eEye REM 1.0 is supported in 4.2x.

Uprade Instructions

The MARS upgrade packages are the primary vehicle for major, minor, and patch software releases. As administrator of the MARS Appliance, you should check the upgrade site regularly for patch upgrades. In addition to addressing high-priority caveats, patch upgrade packages update system inspection rules, event types, and provide the most recent signature support.

For detailed instructions on planning and performing an upgrade or install, refer to Checklist for Upgrading the Appliance Software in the *Install and Setup Guide for Cisco Security MARS 5.x.*

Important Upgrade Notes

To ensure that the upgrade from earlier versions is trouble free, this section contains the notes provided in previous releases according the release number. Please refer to the notes that pertain to the release you are upgrading from and any releases following that one.

Upgrade to 5.2.8 (2591)

CSCsk77372 - 5.2.7, 5.2.8 missing parameter file needed for archiving and restore

Issue: Customers who upgraded from MARS 5.2.4 (2487) to 5.2.7 (2555) and then to 5.2.8 (2590) are missing a parameter file required for the archiving feature.

Verify Issue: To confirm you have upgraded from 5.2.4 (2487) to 5.2.7 (2555) or from 5.2.7 (2555) to 5.2.8 (2590), enter the following command at the command console and check the last line of the output

pnupgrade log

Resolution: A new 5.2.7 (2556) upgrade package and a new 5.2.8 (2591) patch is available for customers who have downloaded and applied the faulty 5.2.7 (2555) and 5.2.8 (2590) upgrade packages. All packages can be downloaded from:

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

To apply these new packages, follow this step:

- If you are running 5.2.8 (2590), download and upgrade to the package named `csmars-5.2.8.2591.pkg`.

  Verify the system is running version 5.2.8 (2591).

Upgrade to 5.2.7 (2556)

Note There were no upgrades to 5.2.5 or 5.2.6; only 5.2.4 directly to 5.2.7.

CSCsk77372 - 5.2.7, 5.2.8 missing parameter file needed for archiving and restore

Issue: Customers who upgraded from MARS 5.2.4 (2487) to 5.2.7 (2555) and then to 5.2.8 (2590) are missing a parameter file required for the archiving feature.

Verify Issue: To confirm you have upgraded from 5.2.4 (2487) to 5.2.7 (2555) or from 5.2.7 (2555) to 5.2.8 (2590), enter the following command at the command console and check the last line of the output

pnupgrade log

Resolution: A new 5.2.7 (2556) upgrade package and a new 5.2.8 (2591) patch is available for customers who have downloaded and applied the faulty 5.2.7 (2555) and 5.2.8 (2590) upgrade packages. All packages can be downloaded from:

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

To apply these new packages, follow the appropriate step:

- If you are running 5.2.4 (2487), when upgrading to 5.2.7, download and upgrade using the package named `csmars-5.2.7.2556.pkg`.

  Verify the system is running version 5.2.7 (2556).

If desired, you can then upgrade to the package named `csmars-5.2.8.2591.pkg`.

- If you are running 5.2.7 (2555), download and upgrade to the package named `csmars-5.2.7.2556.pkg`.

Note The time to upgrade from 5.2.7 (2555) to 5.2.7 (2556) is shorter than the normal because it only patches the files that must be updated.

Verify the system is running version 5.2.7 (2556).

If desired, you can then upgrade to the package named `csmars-5.2.8.2591.pkg`.

Note If the archive was running on the appliance prior to the upgrade, you must manually restart the archive process after this patch is applied. To restart the archive process, click **Start** on the Data Archiving page, which is accessible via Admin > System Maintenance > Data Archiving.

Required Upgrade Path

When upgrading from one software version to another, a prerequisite version is always required. This prerequisite version is the minimum level required to be running on the appliance before you can upgrade to the most recent version. Table 1 identifies the upgrade path that you must follow to reach the minimum level required to upgrade to current version.

Table 1 Upgrade Path Matrix

From Version	Upgrade To	Upgrade Package
5.2.4	5.2.7	csmars-5.2.7.2556.pkg

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.
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 5.2.7, page 7
- Resolved Caveats - Release 5.2.7, page 15
- Resolved Caveats - Releases Prior to 5.2.7, page 17

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 5.2.7

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
CSCsj63552	PN log agent should check ACS config before allowing user to App name
CSCsj45065	linux events from syslog-ng are seen as generic event type on MARS
CSCsj44151	Need to remove replicated system data from the GC
CSCsj33614	MARS SSH discovery of ASA fails if login banner is set
CSCsj31990	pnparser: to avoid flooding log file
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
CSCsi29398	CS-Mars does mitigate to the proper endpoint
CSCsi23209	Some unsupported nfs cause system errors on MARS.
CSCsi18757	CS-MARS - Request to have the "ssldump" command in the MARS CLI.
CSCsi15769	NLS_LANG variable should be updated in environment
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
CSCsi07719	pnlog packaging should be more error resilient during 'pnlog mailto
CSCsi03658	CS-MARS - IOS Discovery via Telnet/SSH fails with $hostname in banner
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
CSCsh89885	Mitigation command not display properly in 4.2.4
CSCsh89445	GUI allow users create rule without putting rule name
CSCsh82939	MARS failed to restart if the hostname is changed after a restore
CSCsh73553	USB Keyboard does not work while re-imaging with DVD
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
CSCsh52537	Repeated upgrades 4.2.2->4.2.3 fills hard drive
CSCsh42151	GUI Summary pg shows #events < #sessions & negative data reduction rate
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

Reference Number	Description
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
CSCsg80475	All incidents purged if event-session partition table is corrupted.
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
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.
CSCsg64119	rule's keyword editor treats NOT as binary rather than unary
CSCsg54313	ORA-01654: unable to extend index on MARS 200
CSCsg47022	CS-MARS - Incorrect Start Times on Retrieved Raw Message Files
CSCsg41549	MARS discovery issues with Loopback IP on IP Unnumbered interfaces.
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
CSCsg20987	CSMARS DTM sdf files are sent with invalid format
CSCsg20408	FW-6-SESS_AUDIT_TRAIL Parsing Error
CSCsg14082	Default query Changed in system defined report
CSCsg13767	SuperV doesn't detect/restart processes
CSCsg08166	Unable to discover ASA 7.0 Error:There is no Error Log for this Device
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
CSCsf31207	Mars doesn't support new/changed FWSM 3.1.3 maintenance release syslogs
CSCsf31121	Exception in Case Management code when deleting a report
CSCsf26715	Inaccuracy in per-context memory utilization for multi-context devices
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
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
CSCse98029	Occasionally corrupted event data enters into MARS database
CSCse91636	MARS - not all columns seen in CSV reports generated using custom column
CSCse82042	Change the Device Type Version for FWSM
CSCse82022	Unable to view reports starting with #sign in csv format

Reference Number	Description
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
CSCse54976	Some incidents are not written to DB
CSCse54808	The time stamp shown by the pndbusage command is incorrect.
CSCse52217	Customer gets pink box in GenericHostDeviceEditManagement.jsp
CSCse45884	LLV query causes client CPU to go to 100%
CSCse42953	CS-Mars - unable to show L2 path when source and destination in same net
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
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
CSCse31722	Cloud toggle only works on first page of reporting devices
CSCse27948	pink box when do query - ORA-01555: snapshot too old exception
CSCse23191	Disable 'No Pager' cmd sent by MARS to PIX, ASA, FWSM firewalls
CSCse21626	Clicking activate is not taking effect
CSCse20593	CSM device type could not be added one time (OK most times)
CSCse18816	UI takes 99% CPU, hanging browser and slowing system while expanding all
CSCse17936	5K Lines Custom Query fails
CSCse13038	CS-Mars - learning of McAfee agents with invalid names
CSCse10945	Summary Page Graphs Spontaneously Change Displayed Size (w/ multi-head)
CSCse09127	Failed load from csv returns incorrect status
CSCse03237	Changes made to GC network groups are not propagated to active LC rules
CSCse03097	CheckPoint LEA record comes to MARS later and later
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
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.
CSCsd61749	pnrestore doesn't restore all of the system config
CSCsd28590	CS-MARS - Inactive Reporting Device Rule is not configurable

Reference Number	Description
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
CSCsc90480	MARS Incident notification options are not configurable
CSCsc78878	snort signature 2570 incorrectly mapped
CSCsc59363	Need improvement to GUI for multi-line rules
CSCsc48498	CS-MARS: Upgrade from 3.4.x fails
CSCsc42396	CS-MARS Viewing IP of grouped sessions throws Exception, no Time var
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
CSCpn03057	Copied rules have shortened year in front, which is confusing (ex. 0
CSCpn03052	JBoss 'OutOfMemoryError ' when accessing Management/Event Management
CSCpn02976	GC:LC - Communication issues after time zone change
CSCpn02973	Not able to downgrade a security analyst to Notification only user
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

Reference Number	Description
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
CSCpn00610	Backend logs can be out of order in the view page
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
CSCsj18388	Apostrophe character in IP Range/Network Name field causes MSIE to hang.
CSCsj11759	Some reports do not generate email alerts
CSCsj11689	errors thrown when archive data to NFS share on a NetApp
CSCsj11201	pnparser: avoid flooding log when errors occur in parsing SNMP traps
CSCsj07565	Increase shared buffer stall thresholds from 2 mins to 5 mins
CSCsj07526	The maximum size for an internal netflow queue is too large
CSCsi71511	http status 500 appears while clicking the incident on the summary page
CSCsi64605	pnparser restarts frequently with sessionization turned on (default)

Reference Number	Description
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
CSCsi28286	GC-LC upgrade to 4.2.4 resulted in Standalone display on LC
CSCsi19227	Some reports/rules/queries match events outside specified IP ranges
CSCsi17607	GC - Zone Model for Auriga 210 showing as 200
CSCsi15258	Accepting the collector, and source ip address as MARS ip address
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
CSCsi00963	CS-MARS Archiving Causes pidof[xxxxx] Messages to Appear on Monitor
CSCsh99201	MARS-Scheduled ranking report with ACTION filter produces empty results
CSCsh93759	Rules/reports with large queries not working
CSCsh88897	race condition in pnparser triage handling caused syslog processing stop
CSCsh83068	Report and query return no results under device type ANY
CSCsh77508	MARS is not displaying CSM icon for access-list syslog with severity 0
CSCsh75216	InLine multiColumn query case attachment Fails
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
CSCsh56931	Rule engine fires only once if only SAME is present in any column
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
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
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
CSCsg86481	CS-MARS parsing error for ASA7.0 msg 302018
CSCsg83055	parsing error for FWSM-n-302003 and FWSM-n-302004
CSCsg73843	GC - Unable to change configuration information (email IP) from GUI
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

Reference Number	Description
CSCsg64704	DNS wasn't configured correctly,Pausing event processing for 40 seconds
CSCsg60114	System error when generating NAC report
CSCsg53084	MARS - WebVPN ACL Parse error event fires on incorrect syslog
CSCsg44725	need to downgrade log level of CSA snmp trap errors in backend log
CSCsg41027	MARS - Retrieve Raw Messages Fails at 0%
CSCsg26225	Graphs/Images do not show up in case related report emails
CSCsg20514	Mars backend processes need to save backtraces on a crash for debugging
CSCsg16843	MARS reporting misleading licensing problem while trying to add a LC.
CSCsg12475	pnarchiver crashed because of extra files under /pnarchvie/CF directory
CSCsg10787	CatOS telnet discovery failing.
CSCsg04079	Lotus Notes client gets JavaScript error with emailed MARS report
CSCsg02749	custom column report generates empty results
CSCsf30116	Event Rate on the Top Destination Port graph is not correct
CSCsf18192	Slow rendering of the GC/LC Summary page
CSCsf06819	vulnerabilities not updated for hosts reported by deleted eEye console
CSCse98046	need to improve db partition rotation strategy
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
CSCse73868	pnrestore command should support end-time argument in the command line
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
CSCse52782	Can't change run-time to day in "Resource Issues: Server - Top Reporting
CSCse45018	MARS is unable to parse NetScreen 5.x syslogs
CSCse39426	frequent superV & pnparser restarts cause log processing to fail
CSCse38615	Bucket_size field in pn_report_result table is negative
CSCse35420	Interface error rate should be separate from discards and unknown protos
CSCse32591	dealing with duplicate hostnames in VA import
CSCse26964	CatOS Syslog %SYS-4-P2_WARN not parsed correctly by MARS
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
CSCse19198	Device Cnf: Changes in Mail Gateway IP doesn't reflect Report/ Notif
CSCse18240	DOC: cs-mars doesn't handle vpn paths
CSCse11258	After group is deleted, items under "All" group not shown
CSCse07425	JVM is using up to 1.5 GB on a GC or LC

Reference Number	Description
CSCse03134	More control is needed over retrieve raw messages and cleanup
CSCsd92285	Security Dev Edit page does not check for existing IP address conflict
CSCsd84094	using rules in query/report definitions
CSCsd74283	changing report-result retention limit
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
CSCsd64438	pnparser crashed at 2.5k/s for relayed syslog and stops receiving events
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
CSCsd22832	Attempt to remove IP subnet from IP Management fails, with error
CSCsd20196	User and System Scheduled Reports fail to display data
CSCsc91572	Multiple target ports in IDS event show up as 'port 0' in query
CSCsc87501	if set IP address to 0.0.0.0 box trying to reboot
CSCsc73832	Drop rule inactive for events received by netflow in CS-MARS
CSCsc58485	5 tuple information missing from downloaded raw log file
CSCsc30107	Cs-Mars - Queries with != in service column don't work
CSCpn03077	GC, sys error when adding a LC which was added to GC already
CSCpn03005	Loading Resource Util report as On-Demand query produces a system error

Resolved Caveats - Release 5.2.7

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

Reference Number	Description
CSCsj55697	Missing McAfee EPO datawork
CSCsj46242	System report "Spyware -Top Hosts" has wrong query
CSCsj29192	Dates lost in the duplicated report
CSCsj22950	Deleted Report should be removed from the available reports list
CSCsj22660	GC: Pink box when compose a batch query with filter
CSCsj20953	'printsb' prints wrong shared buffer "jump counts
CSCsj15204	Pink box when the deleted report is re-add
CSCsj14955	GEN-2:need to prevent cron job tmpwatch from removing MARS files in /tmp
CSCsj13655	Pnparser doesn't use the new SNMP trap port changed in janus.conf
CSCsj11759	Some reports do not generate email alerts

Reference Number	Description
CSCsi99053	pnarchive, corresponsing es, rm, ix files have different time stamp
CSCsi98592	Print netflow capacity drop event information in janus_log as well
CSCsi95375	MARS 210: event parser process memory limit
CSCsi95117	changes needed in areas for introduce of report status=64
CSCsi95086	report deletion design changes
CSCsi94282	reports can have the same names with diffs on extra blank spaces
CSCsi90577	"scripts" directory doesn't exist on cygnus
CSCsi86634	Need schema for 5.2.7 set to 05_2_70
CSCsi80780	swap partition is not fully used
CSCsi79506	Oracle generates large 1.3G listener.trc file
CSCsi72733	pnparser dies if too much traffic is sent
CSCsi72346	discover process dies when doing scheduled discovery
CSCsi70352	Sync LC will cause the GC IPs pushed back to the GC
CSCsi64918	Oracle 10g support
CSCsi64913	Snort 2.6 Support
CSCsi64605	pnparser restarts frequently with sessionization turned on (default)
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
CSCsi31569	csips process restarts very frequently
CSCsi27709	The datawork script "check.sh" takes a long time to complete
CSCsi19227	Some reports/rules/queries match events outside specified IP ranges
CSCsi12240	Pink box on Summary page of GC when cases are active
CSCsi04306	need to add CPU check for csips, csiosips, and cswin
CSCsi03686	CS-MARS - HTML/XML tags are not escaped when displaying packet context
CSCsh99201	MARS-Scheduled ranking report with ACTION filter produces empty results
CSCsh93759	Rules/reports with large queries not working
CSCsh85870	Admin->Maintenance->Retreive Raw Message causes out of memory error
CSCsh72929	OutOfMemoryError/Bad performance in RULES/QUERY- large configuration
CSCsh69765	CLI date/time/ntp commands should reboot if time change exceeds 30 mins
CSCsh64155	MARS is not sending all the parameters to CSM for ASA acl syslog
CSCsh56931	Rule engine fires only once if only SAME is present in any column
CSCsh40698	VPN GroupName and Username disappeared from its raw event message
CSCsh34170	Change/Modify report needs to purge existing reports
CSCsh14070	CS-Mars - Microsoft Misspelled in VA section
CSCsg86481	CS-MARS parsing error for ASA7.0 msg 302018

Reference Number	Description
CSCsg83055	parsing error for FWSM-n-302003 and FWSM-n-302004
CSCsg66801	Activity: All Events and NetFlow report chart is missing on summary page
CSCsg64951	Certain ASA 7.0 syslogs do not get parsed by MARS
CSCsg64704	DNS wasn't configured correctly,Pausing event processing for 40 seconds
CSCsg52502	FWSM 3.1: parsing does not resolve predefined name to IP in Auriga-2
CSCsg44725	need to downgrade log level of CSA snmp trap errors in backend log
CSCsg39552	Certain FWSM 2.3 syslogs give parsing errors/unknown event type in 4.2.2
CSCsg26225	Graphs/Images do not show up in case related report emails
CSCsg10787	CatOS telnet discovery failing.
CSCsg04079	Lotus Notes client gets JavaScript error with emailed MARS report
CSCsf18192	Slow rendering of the GC/LC Summary page
CSCsf06819	vulnerabilities not updated for hosts reported by deleted eEye console
CSCse84962	eEye: MARS does not remove resolved vulnerabilities from host info
CSCse60240	CS-Mars - report for old events include real-time events
CSCse53856	Got "Error on page" when displaying packet data from IDS device
CSCse39426	frequent superV & pnparser restarts cause log processing to fail
CSCse23051	viewing report of query type of MAC addresses report got pink box
CSCsd88284	optimizing incident inserts in DbIncidentLoaderSrv
CSCsd74283	changing report-result retention limit
CSCsd69063	Reported User with single-quote (') causes oracle error
CSCsd48097	Event processing may stop if pnparser creates shared buffers first
CSCsd31161	net-snmp config files are missing on machines running 4.3.1 (5014)
CSCsc70982	change the button string on the false/positive column to "Tune
CSCsc47210	inline process srv could crash

Resolved Caveats - Releases Prior to 5.2.7

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