Release Notes for Cisco Security MARS Appliance 5.3.1

Revised: October 30, 2007, OL-14669-01

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 5.3.1 running on any supported Local Controller or Global Controller as defined in Supported Hardware, page 2. They provide the following information:

Introduction

Version 5.3.1 is now available as an upgrade of 5.2.8 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 5.3.x versions to MARS 20, 20R, 50, 100, 100e, 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 5.3.1 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 5.3.1 supports the following Cisco Security MARS Appliance models:

Local Controller Appliances

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

Global Controller Appliances

- Cisco Security MARS GC2R (CS-MARS-GC2R-K9)
- Cisco Security MARS GC2 (CS-MARS-GC2-K9)

New Features

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

Data Migration Support

Beginning with this release, you can migrate configuration and event data from a MARS Appliance running 4.x to a newer model running 5.x. For detailed instruction on how to perform this operation, see *Migrating Data from Cisco Security MARS 4.x to 5.3.x.* at the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/5.3/user/guide/local_controller/authen.html#wp1198343

Centralized Password Management—External AAA Server Support

External Authentication, Authorization, and Auditing (AAA) servers can now act as the authentication mechanism for MARS Appliance GUI logins (username and password). Previously, each MARS Appliance authenticated login name/password combinations with the appliance's local user database. Release 5.3.1 supports the following external RADIUS AAA servers:

- Cisco Secure Access Control Server (ACS)
- Microsoft Internet Authentication Service (IAS) Server
- Juniper Networks Steel belted RADIUS

Further Information is available at the following URL:
http://www.cisco.com/en/US/docs/security/security_management/cs-mars/5.3/user/guide/local_controller/authen.html

Account Locking—Login Security

Previously, MARS Appliances permitted an unlimited number of login attempts. With Release 5.3.1, the adminstrator can configure the GUI to lock after a specified number of failed login attempts, or can configure the GUI to never lock. To set the Account Lockout Policy, navigate to the AAA configuration page (**Admin > System Setup > Authentication Configuration**).

The administrator can unlock accounts form the User Management page (**Management > User Management**), or with the new **unlock** CLI command.

Note Per Open Caveat CSCsk31615 in Release 5.3.1, when MARS fails in an attempt to connect to a specified external AAA server, MARS behaves as if the user had performed a failed login. This can result in users being locked out of the GUI even when they are entering the correct login name and password combination. For example, if three AAA servers are specified, and all three attempts to connect to them fail, and the Maximum Login Failures parameter is set to 3, the user will be locked out of the GUI with one valid login attempt. This behavior will change in a future release.

Further information is available at the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/5.3/user/guide/local_controller/authen.html#wp1198343

Monitoring Global Controller Connection Status from the Local Controller

Previously, the connection status between a Local Controller and a Global Controller was reported on the Global Controller's Zone Controller Information page (**Admin > System Setup > Local Controller Management**).

With Release 5.3.1, the Local Controller now generates syslogs to record communication problems caused by the following events:

- Local Controller cannot connect to the Global Controller
- Local Controller certificate is not on the Global Controller or vice versa
- Local Controller and Global Controller are operating with incompatible MARS release versions

Release 5.3.1 defines seven new events, three new system rules, and two new system reports on the Local Controller to monitor the connection status with the Global Controller.

Further information is available at the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/5.3/user/guide/global_controller/gccfg.html#wp1055211

GUI and CLI Timeout Interval

Previously, the GUI would timeout after 30 minutes of inactivity. With Release 5.3.1, the timeout interval for the GUI can be set at 15, 30 (default), 45, and 60 minutes, or as Never (never will timeout). Different GUI timeout intervals can be set for the Administrator, Security Analyst. and Operator roles. The Administrator parameter also sets the CLI timeout.

To access the Timeout Configuration page, navigate to **Admin > System Parameters > Timeout Settings**.

Support for Cisco IPS 6.0 Dynamic Signature Updates

This feature downloads new signatures from CCO and correctly process and categorize received events that match those signatures, which includes them in inspection rules and reports. These updates provide event normalization and event group mapping, and they enable your MARS Appliance to parse day zero signatures from the IPS devices.

By default, this feature is enabled and requires you to configure it. If you do not configure it, the following rule fires:

```
System Rule: CS-MARS IPS Signature Update Failure
```

This rule fires daily until you configure the feature. To address the issue identify by this firing rule, do one of the following:

- Specify the username and password pair to use when pulling the signature updates from CCO.
- Specify a local server where the MARS-IPS packages reside in the URL for Signature update field.
- Disable the feature.

For information on configuring the feature, see IPS Signature Dynamic Update Settings.

Miscellaneous Changes and Enhancements

The following changes and enhancements exist in 5.3.1:

- **Global Controller-to-Local Controller Communication Enhancements.** Enhancements include more efficient data batches, reduced transfer times, and a prioritization on recent data. If a data backlog occurs due to a Global Controller-to-Local Controller disconnect, the Local Controller sends recent data first and stays in sync with new data coming in. The Local Controller catches up with older data over time.
- **Syslog Forwarding**. Designate a syslog collector and forward syslog messages received from one or more IP addresses to that collector. See the **syslogrelay setcollector**,**syslogrelay src**, and **syslogrelay list** commands in *Appendix A: Command Reference* in the *Install and Setup Guide for Cisco Security MARS*. See “Syslog Relay Support” in *Chapter 2: Reporting and Mitigation Devices Overview* of the *User Guide for Cisco Security MARS Local Controller.*
- **Password Management Enhancement.** Non-administrative users can change the password associated with their account. Previously, editing a MARS user was considered an administrative task and limited to those accounts with the admin role.
- **Raw Message Log Enhancement.** To view and delete queries in the local cache, click the **View Cache** button on the Retrieve Raw Messages page accessed from **Admin > System Maintenance > Retrieve Raw Messages**.Previously, queries were purged automatically every two weeks; this feature helps avoid disk space shortages that could occur before that period elapsed.

- **GC2R Support.** The 4.3.1 and 5.3.1 releases are interoperable, allowing the GC2R to manage Local Controllers running 4.3.1 on the following models: MARS 20R, MARS 20, and MARS 50.
- **Enhanced Cisco Device Support**:
  - IPS 6.0
  - PIX / ASA 7.2
  - CSA 5.0, 5.1, and 5.2
  - Cisco IOS Release 12.4(11)T through IOS Release 12.4(11)T4
  - FWSM 3.1.3 and 3.1.5
- **Enhanced 3rd-Party Device Support.**
  - ISS Site Protector 2.0
  - CheckPoint R61, R62, and R65.
- **Update to intrusion prevention, and intrusion detection, and vulnerability assessment signature sets.** This release includes new vendor signatures, updating the 3rd-party signature support. For more information on the updates, see New Vendor Signatures, page 5
- **Bug fixes.** For the list of resolved issues, see Resolved Caveats - Release 5.3.1, page 17.

New Vendor Signatures

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

Revised in 5.3.1	Product	Signature Version Supported
Intrusion Prevention and Detection Signatures		
Yes	Cisco IDS 4.0, Cisco IPS 5.x, Cisco IOS 12.2	Current through S299 signature release.
Yes	Snort NIDS 2.6.1	Current through the July 7, 2007 signature release
No	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
No	McAfee IntruShield NIDS 1.8 McAfee Network Intruvert v 2.1.9.104	2.1.68.5 Release date: June 12, 2007
Yes	McAfee Entercept HIDS 6.x	Current through the August 21, 2007 signature release.
Yes	CheckPoint Application Intelligence (VPN-1 NG with Application Intelligence R55)	Current through the August 6, 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 July 3, 2007 signature release.
Yes	Symantec NIDS, v 4.0	Signature package: 84 Release date: July 15, 2007

Revised in 5.3.1	Product	Signature Version Supported
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.
Vulnerability Scanner Signatures		
Yes	Qualys QualysGuard 3.x, 4.7.161-1	Current through the August 17, 2007 signature release.
Yes	E-Eye, Retina Scanner Vulnerability Software, version 5.6[1]	Current through the August 20, 2007 signature release.
Yes	Foundstone, version 4.x	Current through the August 23, 2007 signature release.
Yes	Common Vulnerabilities and Exposures (CVE) Database	Current with the August 15, 2007 definition update.

1. eEye REM 1.0 is supported in 4.2x.

Upgrade 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 5.3.1

Beginning with the 4.3.1 and 5.3.1 releases, the dynamic IPS signature updates (if enabled) is an aspect of the version of software running on a MARS Appliance. Therefore, in addition to running the same MARS software versions on the Global Controller and Local Controller, the IPS signature version must match or the communications fail.

In a Global Controller-Local Controller deployment, configure the dynamic signature URL and all relevant settings on the Global Controller. When the Global Controller pulls the new signatures from CCO, all managed Local Controllers download the new signatures from the Global Controller.

In addition, CSCsk90015 states that any reporting device representing a Cisco ACS 3.x device that exists prior to the 5.3.1 upgrade is deleted during the upgrade. To resolve the issue after upgrade, you must the remove the reporting device from the host and re-add that device again as Cisco Secure ACS 3.x .

An example process is as follows:

1. Click **Admin > Security and Monitor Devices**, select the host with Cisco ACS 3.x as a reporting application and click **Edit**.
2. Select the **Reporting Applications** tab, and then blank link and click **Remove**.

3. After removing the blank link, re-add Cisco Secure ACS 3.x application to that host and click **Activate**.

Upgrade to 5.2.8

The upgrade is from 5.2.7 to 5.2.8. No important notes exist for this release.

Upgrade to 5.2.7

The upgrade is from 5.2.4 to 5.2.7; no 5.2.5 or 5.2.6 releases exist.

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.pkg
5.2.7	5.2.8	csmars-5.2.8.pkg
5.2.8	5.3.1	csmars-5.3.1.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 5.3.1, page 9
- Resolved Caveats - Release 5.3.1, page 17
- Resolved Caveats - Releases Prior to 5.3.1, page 28

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 5.3.1

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
CSCsk90015	Cisco ACS 3.x not accessible after upgrade to MARS x.3.1
CSCsk60311	Mars - Option to check logs pulling status
CSCsk59030	MARS OpenSSH GSSAPIDelegateCredentials vulnerability
CSCsk57521	Test Connectivity to CSM fails when CSM password contains special chars
CSCsk51397	Adding many incidents to the case slows down the MARS gui performance
CSCsk49710	User Guide - NetScreen device configuring syslog screenshot incorrect
CSCsk45704	User account always display locked
CSCsk43710	Gen2 GC miss Genl LC's info on the license page
CSCsk42805	Statistics backlog creates high CPU condition
CSCsk39645	GUI doesn't check duplicate agent ip address when adding application
CSCsk31615	Should not increase the number of failure for AAA server unaccessible
CSCsk27999	Java error when clicking on Configuration Information page
CSCsk27276	MARS: Isolated Networks in Topology due to 'ip unnumbered' Interface
CSCsk26308	pink error when listing devices while scalability script running
CSCsk21865	LC/GC comm broken due to java io stream header corruption exception
CSCsk19730	Null XML_KEY_VALUE XML causes rule to go inactive on LC/GC sync
CSCsk17861	Mars released DVD contains GUI management source codes
CSCsk12489	operator role can not resubmit report
CSCsk12156	Configuration Sync (GC --> LC) can have parallel threads doing dupe work
CSCsk11592	ids didn't get monitored networks from msfc if discover ids first
CSCsk08028	Real time multi column query is not working.
CSCsk06363	System Rule: Resource Issue: CS-MARS should include drop counts events
CSCsk04282	MARS failed to import 1000 hosts vulnerablilty information
CSCsk03722	Test Connectivity returning error
CSCsk03186	Error during discovery of Netscreen SSG5 w/ ScreenOS 5.0
CSCsk03022	After LC was deleted from GC, GC-LC communication goes on forever
CSCsk02989	GC is not usable when LC has lots of deleted devices
CSCsk02261	XPATH is change to find open ports information from QG 5.0 xml file

Reference Number	Description
CSCsk62114	Wrong spelling Error Messages
CSCsk62697	IPS6x is not supported in seed file import in 4.3.1/5.3.1
CSCsj96747	Networks and Groups propogated 2 LC are deleted after its removed fr GC
CSCsj96592	Adding LC with version lower than 4.3.1 should version mismatch err
CSCsj90875	Inline/Batch query: result mismatch on Matched Rule Ranking
CSCsj90505	Inline/Batch query not match on NAT connection report
CSCsj89299	MARS unable to discover ASA through ssh using DES
CSCsj87207	GUI cannot show the full topology because of constant process crash
CSCsj73189	IOS and IPS certificates aren't deleted when the device is deleted
CSCsj71119	Loading devices from seed file didn't populate interface info
CSCsj69985	Syslogrelay is accepting same IP for both source and collector
CSCsj68087	MARS Discovery fails to take the context information of ASA from 7.2-7.0
CSCsj67626	Raw message query type schedule report missing some raw message events
CSCsj67037	pnparser / postfire / process_event_srv crashed in func test
CSCsj66955	scheduled discovery is scheduled at wrong time
CSCsj63552	PN log agent should check ACS config before allowing user to App name
CSCsj57812	Mars unable to parse CP R61 Hide NAT behind gateway config
CSCsj57315	Mars doesn't parse and store CP R61 User/Client/Session auth rules
CSCsj51240	Paging does not work for report right after adding it to a case.
CSCsj51181	Batch query submitted from a GC to LC is still in progress after two day
CSCsj42467	LC not showing up on certificate page
CSCsj41168	Error when trying to accept new sensor certificate
CSCsj33614	MARS SSH discovery of ASA fails if login banner is set
CSCsj31990	pnparser: to avoid flooding log file
CSCsj30328	Hosts not loading when existing hosts slected.
CSCsj29441	rpcclient2 abnormal uder 1050 windows devices env
CSCsj28376	Box may not be able to reboot after recovery, under certain conditions
CSCsj23845	The Action filter doesn't work if it is not associated with incidents
CSCsj20697	LC did not get added to GC so unable to generate syslogs.
CSCsj15512	Update reports when handling deletion of hosts
CSCsj11689	errors thrown when archive data to NFS share on a NetApp
CSCsi96921	IPSDynamicSigUpdate attempts to connect to CCO with no credentials
CSCsi95074	low-traffic bytes ranking report causes process_inlinerep_srv to restart
CSCsi93594	Pnparser stops processing each time it tries to load the topology
CSCsi93283	Mismatch between query and report results for source port ranking.
CSCsi91734	Mismatch in results between query and report for All Matching Events
CSCsi89837	MARS does not recognize SNMP traps from IPS device

Reference Number	Description
CSCsi86420	with 60% event rate capacity, query events ranked by time takes 20 min
CSCsi76255	Custom log template pattern messed up when add a LC to GC
CSCsi69310	security hole happens if users close browsers without click logout
CSCsi68126	For multiple context mode, inbound/outbound error reports are incorrect.
CSCsi65713	Index needs to be removed for the pn_report_result table
CSCsi62384	The performace test kills all the process during the weekend run
CSCsi53831	performace test causes all the process restarted
CSCsi52731	mars reboots w/o asking for confirmation after user clicked cfg update
CSCsi51999	Edit SW based Application device need submit twice
CSCsi50058	GC not merging the same reporting device from LCs
CSCsi50024	IPS is not visible in Global Zone Hot Spor Graph
CSCsi49474	Mismatch results between query and report (custom column)
CSCsi49419	The application hangs, while getting the results for a query.
CSCsi49396	Mismatch in results between query & report when query based on desti. IP
CSCsi49330	Mismatch in results between query and report when query is based on user
CSCsi49285	Mismatch in results between query and report.
CSCsi32559	Able to run a query when the limit is reached
CSCsi32553	MARS Client CPU hits 95-100% during Real-Time (raw events) query
CSCsi31867	csips crashes due to memory corruption
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
CSCsi15258	Accepting the collector, and source ip address as MARS ip address
CSCsi13100	gui.sh dev build makes different JBOSS web.xml than make release
CSCsi11963	MARS 4.2.4 not parsing IOS Router NAT properly
CSCsi11312	pn_incident_log and pn_report_log should be archived
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.
CSCsi07719	pnlog packaging should be more error resilient during 'pnlog mailto
CSCsi07186	User can input unsupported characters in AAA device name
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
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
CSCsh89445	GUI allow users create rule without putting rule name
CSCsh82939	MARS failed to restart if the hostname is changed after a restore

Reference Number	Description
CSCsh77508	MARS is not displaying CSM icon for access-list syslog with severity 0
CSCsh73553	USB Keyboard does not work while re-imaging with DVD
CSCsh58754	Lots of oracle files on HD can cause upgrade failure, succeeds on retry
CSCsh57236	Unknown Reporting Device was missing on GC's DB pn_device table
CSCsh52537	Repeated upgrades of oracle fills hard drive
CSCsh44351	CSM multiple hostname matches failed to return multiple hosts
CSCsh41920	No warning for Invalid entry to Query maximum number of rows returned.
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
CSCsh14454	server.log can grow unbounded with in a single day
CSCsh00013	Case Management: history does indicate change of ownership
CSCsg98026	pnlogagent causes acs log files to add (01) to file name
CSCsg91816	Query for ICMP port 0 shows UDP/TCP results
CSCsg82600	some syslog results in unknownDET with 'Activate
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
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
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
CSCsg12475	pnarchiver crashed because of extra files under /pnarchvie/CF directory
CSCsg08166	Unable to discover ASA 7.0 Error:There is no Error Log for this Device
CSCsg02749	custom column report generates empty results
CSCsf99844	wrong values for current connections using CLI "show resource usage

Reference Number	Description
CSCsf99767	provide encoding selection for adding agent to device/host
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
CSCsf27568	keyword search query can't display big-5 encoding raw msg
CSCsf26715	Inaccuracy in per-context memory utilization for multi-context devices
CSCsf15781	Database table columns do not match with the archive file columns
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
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
CSCse85972	Unresolved symbol in Java build (though didnot stop building)
CSCse85564	Cannot add devices to a report which has more than 35 devices.
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
CSCse73868	pnrestore command should support end-time argument in the command line
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.
CSCse51642	IPlanet Unknown Device Event Type Parsing Error
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
CSCse38615	Bucket_size field in pn_report_result table is negative
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

Reference Number	Description
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
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
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
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.
CSCsd74681	OS 4.0: FlexLM License
CSCsd64438	pnparser crashed at 2.5k/s for relayed syslog and stops receiving events
CSCsd61749	pnrestore doesn't restore all of the system config
CSCsd48544	port 8444 required for GC/LC communication
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
CSCsc59363	Need improvement to GUI for multi-line rules
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

Reference Number	Description
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
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
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
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

Reference Number	Description
CSCpn01045	Archiving: Need better error message
CSCpn00908	"Domain" in Configuration page - no use
CSCpn00586	nasl message text needs to be changed
CSCpn00455	Graph doesn't refresh when a cloud is renamed
CSCpn00293	using TAB in editing fields
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 5.3.1

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

Reference Number	Description
CSCsk41641	5 nasl scripts' references need to be removed from bigfiles
CSCsk37063	LLV Query Resume button does nothing
CSCsk28367	Datawork merge of 4.3.1 data into 5.3.1
CSCsk27325	KeywordQuerySrv crashed because of thread safety issue of posix regex
CSCsk25344	Migration: Data Import fails on machine upgraded to 5.3.1 from 5.2.7
CSCsk24427	query for raw message hangs when device name has charactor "@
CSCsk20580	After pnrestore Oracle gets fatal internal error
CSCsk12572	Datawork merge from 4.2.8 to BOOTES(4.3.1)
CSCsk12317	IPS signature status incorrect
CSCsk12130	Editing system rules before upgrading can cause LC/GC sync problems
CSCsk02952	High rate events/netflows with large topo can be dropped on an activate
CSCsj98279	IPS Autoupdate CCO URL
CSCsj97806	Need to assign a raw msg file ID to 4.x.x archives
CSCsj97614	pnimp on Cygnus failed to report date format error
CSCsj92134	Raw message retrieval from NFS thrown an exception
CSCsj87412	Synchronization doesnot happen between LC and GC (upgrade problem)
CSCsj86127	Merge issue with datawork in 4.3.1/5.3.1 branch
CSCsj83596	Restore and migration for GC failed, one extra data field needed.
CSCsj81545	Netflow processing has an unnecessary STL call that uses 20% CPU
CSCsj80689	error on the console in the beginning of pnrestore
CSCsj74575	Import Data command processes data before date specified

Reference Number	Description
CSCsj74155	Cannot Retrive Raw Messages while sending PIX72,ASA72 and SNORT messages
CSCsj73189	IOS and IPS certificates aren't deleted when the device is deleted
CSCsj63436	IPS Signature Download From CCO failed
CSCsj58986	ORACLE not available error, when applying hostname after fresh image
CSCsj56231	Oracle raw message not retrieved
CSCsj55791	ACS device type not showing up
CSCsj55344	Pink box on the Batch query page
CSCsj54055	GUI doesn't prompt for different/new CSM SSL cert
CSCsj53807	Wrong results for event filter != 'ET group' in scheduled reports/LLV
CSCsj52468	Parsing not happening for Materialized events of Oracle 10g
CSCsj51496	Scheduled Report of Rpt Device Type Ranking generate empty result
CSCsj47615	Mars is unable to retrieve logs from CheckPoint NGX CLMs
CSCsj46242	System report "Spyware -Top Hosts" has wrong query
CSCsj46089	parsing error for pix/asa 302003 , 302004
CSCsj45065	linux events from syslog-ng are seen as generic event type on MARS
CSCsj44151	Need to remove replicated system data from the GC
CSCsj44134	jboss stopped after mode 3 pnrestore
CSCsj43393	Getting "Unknown character = (35|#)" as first line while exec cmd in pn
CSCsj42390	enh: trim leading/trailing spaces in reported user, wksn, domain names
CSCsj40715	Report results could be delayed in synchronizing between LC and GC
CSCsj37565	remove Linux OS info from 'show healthinfo' output
CSCsj34826	esti_time: some error messages appear
CSCsj33630	Sending zero length message causes process flooding system logs
CSCsj33016	Timeout feature is not working as expected.
CSCsj29432	need to purge inactivated report data
CSCsj29192	Dates lost in the duplicated report
CSCsj28384	After migration, Oracle may not be able to start
CSCsj23876	Configuration Import Fails to Run
CSCsj23003	Event Type Info contains invalid characters
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
CSCsj19220	Unable to download signature files when a proxy is configured
CSCsj18798	Trigger Packet not parsed correctly in ips 6.0 events
CSCsj18753	MARS not parsing source ip, dest ip from 6.0 ips event
CSCsj18388	Apostrophe character in IP Range/Network Name field causes MSIE to hang.
CSCsj16996	Arbitrary Log Size Feature Broken in Cygnus

Reference Number	Description
CSCsj16584	GC: Notification user cannot be added
CSCsj16089	Event 103006 and 103007 of FWSM 3.1.5 not handled properly
CSCsj15714	Collect topology/configuration information in logs for debugging
CSCsj15236	Top Rule Fired report is missing in the Summary page.
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
CSCsj13115	redudant malloc per event rxd in pnparser
CSCsj11871	Mars OS recovery
CSCsj11768	Add Info level logging for debugging topo synchronization
CSCsj11759	Some reports do not generate email alerts
CSCsj11201	pnparser: avoid flooding log when errors occur in parsing SNMP traps
CSCsj09479	superV should cause processes to dump a backtrace before restarting them
CSCsj07565	Increase shared buffer stall thresholds from 2 mins to 5 mins
CSCsj07526	The maximum size for an internal netflow queue is too large
CSCsj07275	Incorrect mapping of an attempted ftp login event
CSCsj06461	Web server log events do not update the received event count
CSCsj02168	Problem upgrading from 5.2.4 to 5.3.1
CSCsj02153	cannot add nm-cids module to ios router
CSCsj00904	Cannot change versions on IPS devices
CSCsi99075	pnrestore exited after getting an error from restoring es files
CSCsi99053	pnarchive, corresponsing es, rm, ix files have different time stamp
CSCsi98818	pn_agent.agent_subtype not getting set for IPS 5.x modules of ASA
CSCsi98607	if AAA server is not reachable, user accounts never lock up
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
CSCsi95047	Upgrade script related to Auto Update needs to be included in Cygnus
CSCsi94282	reports can have the same names with diffs on extra blank spaces
CSCsi94146	error restoring rr files
CSCsi92088	csips process stops running
CSCsi90577	"scripts" directory doesn't exist on cygnus
CSCsi89028	Support for FWSM 3.1.5
CSCsi86975	Version modified after import
CSCsi86351	superV falsely restarted pnparser when timestamp file got removed
CSCsi84817	MARS 4.2.5 - not categorising Windows Security event ID 672 properly

Reference Number	Description
CSCsi82960	Add Oracle RDA tool into system image
CSCsi82387	System Error after deleting NetG referenced by a Rule
CSCsi81458	Estimated time to import is different from Reported time during Import
CSCsi80781	Priority field incorrectly updated for an existing event type
CSCsi80780	swap partition is not fully used
CSCsi79506	Oracle generates large 1.3G listener.trc file
CSCsi79438	Percentages in Summary page often add to 99%, not 100%
CSCsi77753	Improper grammer in error message
CSCsi77558	ET exists without DET
CSCsi77501	Audit Log transactions for NetG change failing at LC
CSCsi75622	Enh: LC dramatic perf improvement for false pos if many devices
CSCsi74233	Cygnus builds missing encrypted gdb debug?
CSCsi74080	correct the debug log levels for certain syslog relay related messages
CSCsi73935	Last Updated time updates every time
CSCsi72733	pnparser dies if too much traffic is sent
CSCsi72346	discover process dies when doing scheduled discovery
CSCsi71703	csips restarts on Cygnus mars
CSCsi71511	http status 500 appears while clicking the incident on the summary page
CSCsi71456	Test Connectivity fails when MARS times out
CSCsi71176	When AAA is enabled, users can not change pnadmin email address
CSCsi70352	Sync LC will cause the GC IPs pushed back to the GC
CSCsi68698	Reported User GUI notification for GC rule is broken
CSCsi68051	GUI FTP upgrade fails due to incorrectly calling the CLI pnupgrade cmd
CSCsi65736	Getting error when clicked on Resume button
CSCsi65719	Able to see networks which are not part of valid network
CSCsi64918	Oracle 10g support
CSCsi64913	Snort 2.6 Support
CSCsi64679	Bootes: PIX7.2 8 syslogs have parsing error or unknown event
CSCsi64605	pnparser restarts frequently with sessionization turned on (default)
CSCsi64138	Upgrade/installation script needs to call post_cleanup.sql
CSCsi64090	parsing set wrong dest ports for some CheckPoint Generic Events
CSCsi60690	mars leaves open ips subscription after removing ips from gui
CSCsi60547	Long LC/GC disconnect leads to report sync problem
CSCsi60506	deletion of host/ip addr/iprange/network/network grp will affect report
CSCsi60491	delete devices will affect report if the report includes these devices
CSCsi60217	Sending report records and firing events from LC to GC is slow.
CSCsi60206	Should set protocol = tcp, dest port = 443 in GUI login event msg

Reference Number	Description
CSCsi59191	too much IDS log flooding when doing performance testing
CSCsi57369	schema from_to scripts incorrect for autoupdate process
CSCsi57271	able to browse GUI without loading license file
CSCsi57229	Upgrade doesn't set log level on autoupdate after upgrade
CSCsi56045	missing one db script inside the installation package
CSCsi54570	tzdata update for Turkey, Mongolia, Cuba, Resolute, Nunavut
CSCsi54173	Signature package name is missing when download is failed
CSCsi52687	pnrestore does not restore event/session/incident
CSCsi52622	postfire lags behind due to doing large amount of NetBios name updating
CSCsi52495	Always Prompt for SSL cert, Test Conn removes IPS' Monitored Nets
CSCsi52293	pnadmin cannot login to CLI/GUI after changing its email address
CSCsi52093	"confirmation" field in the shared secret field for RADIUS
CSCsi52086	the syslog for "pnadmin" login should show "Local authentication
CSCsi51994	One system rule has wrong description
CSCsi49997	Attack Diagram - Large Graph issue
CSCsi48883	Cygnus sanity test: createdb.log errors and permissions
CSCsi48259	GC allows to suspend a LC in "Not Responding " state
CSCsi47531	IPS's "Test connectivity" doesn't discover the "Monitoring networks
CSCsi45619	Pink box when run NAC report on firing events
CSCsi42780	GUI timeout feature is not working for the real time queries.
CSCsi42488	CF be archived daily regardless archiving is turned on or not
CSCsi41173	If error occurs sending config change to LC, no other config sent
CSCsi39264	Cannot Configure an IDSM Module to PULL IPS logs
CSCsi35209	Cannot Add IPS 5.x/6.x as a ASA module
CSCsi32777	Configuring many events in drop rule can cause pink box error
CSCsi31569	csips process restarts very frequently
CSCsi31277	autoupdate process stopped on GC
CSCsi30271	system rule needs updating for new internal events due to syslog relay
CSCsi30168	BOOTES: Add AAA support on MARS
CSCsi30110	Exception happened when clicking details ... button
CSCsi29946	Merge changes from Bootes branch to Cygnus branch
CSCsi29930	GUI: remove feedback in the GUI bottom
CSCsi29451	Different Version of LC-GC should be compatible
CSCsi28286	GC-LC upgrade to 4.2.4 resulted in Standalone display on LC
CSCsi27957	LC generats Software versions syslog even when GC-LC have same version
CSCsi27939	Post-Bootes Upgrade script error reporting
CSCsi27891	'hostname' command should update workstation in mars reported users

Reference Number	Description
CSCsi26753	"Path/Mitigation" should be "N/A" for internal syslog msg
CSCsi24098	AAA auth user account locked message is inconsistent
CSCsi24077	Event "password remains default" is generated with wrong event type
CSCsi24013	ADMIN > Custom Setup > User Defined ... does not set subtab
CSCsi22877	wrong message is generated while doing non admin user unlock from GUI
CSCsi22689	wrong message is generated while CS_MARS failed to connect to AAA server
CSCsi22662	wrong message is generated while unlocking admin user from CLI
CSCsi21278	GC/LC does not time out with 15 minutes and 30 minutes setting
CSCsi19423	Bootes: Change Version doesn't work for ASA7.0/7.2
CSCsi19227	Some reports/rules/queries match events outside specified IP ranges
CSCsi17782	Some OS/application setting not archived.
CSCsi17607	GC - Zone Model for Auriga 210 showing as 200
CSCsi15237	Taking the MARS IP address 127.0.0.1 and 10.1.1.255 as collector IP add
CSCsi14586	Mars generated syslogs with mars as source IP do not trigger incidents
CSCsi12240	Pink box on Summary page of GC when cases are active
CSCsi11225	pn_report_group2report is not included in cf archive (and should be)
CSCsi10795	MARS didn't pull syslog from generic window
CSCsi10692	FWSM2.3: protocol is missing for FWSM-6-106025
CSCsi08151	Incidents should not be pushed to GC when LC/GC has incompatible version
CSCsi08144	No syslog generated when network cable is unpluged from GC
CSCsi07641	Allow cloning of reports to allow more rapid report creation
CSCsi07175	Erroneous install/deployment gets wrong error messages
CSCsi07165	Login failure window has misleading link name
CSCsi06130	GUI timed out too quickly in query page
CSCsi05642	Admin Tab : Raw message retrieval process is very Slow.
CSCsi04404	auto-update required during data import process
CSCsi04306	need to add CPU check for csips, csiosips, and cswin
CSCsi03807	Make DB Changes for IPS Signature Autoupdate
CSCsi03686	CS-MARS - HTML/XML tags are not escaped when displaying packet context
CSCsi02718	Checkpoint module removal triggered AAA
CSCsi02638	Need to implement deleteCmd in DBAPI class DbEventType2App.java
CSCsi00493	Implement IPS Dynamic signature support
CSCsh99201	MARS-Scheduled ranking report with ACTION filter produces empty results
CSCsh95942	data migration from Gen1 to Gen2
CSCsh95924	PIX/ASA 7.2 support in MARS
CSCsh95836	Add utility SQL scripts to installation for customer support
CSCsh93759	Rules/reports with large queries not working

Reference Number	Description
CSCsh93364	Creating a Case gets (harmless) ClassNotFoundException in JBOSS log
CSCsh93354	BOOTES: compiler optimization for pix 7.2 parser used up memory, stopped
CSCsh89885	Mitigation command not display properly in 4.2.4
CSCsh88897	race condition in pnparser triage handling caused syslog processing stop
CSCsh88639	Add DB utility methods (log, long running query stats...)
CSCsh83470	DB function to convert unix time to readable string for convenience
CSCsh83184	Device added as an Enterasys Dragon 6 does not show in Full Topology map
CSCsh83068	Report and query return no results under device type ANY
CSCsh82764	GC: Device-related Interface data left in DB after LC deleted
CSCsh81718	Raidstatus output: missing rebuild status for one drive.
CSCsh80210	Generate locking and unlocking events.
CSCsh78668	Extra ';' following '>' in keyword query result
CSCsh78039	Keyword search returned results without highlight
CSCsh77146	Do not delete LC certificate from the GC when the zone is deleted
CSCsh75216	InLine multiColumn query case attachment Fails
CSCsh72929	OutOfMemoryError/Bad performance in RULES/QUERY- large configuration
CSCsh71637	re-add a deleted CSA console may cause the submit page hang
CSCsh69765	CLI date/time/ntp commands should reboot if time change exceeds 30 mins
CSCsh68717	GUI Should change: Cisco ACS --> Cisco Secure ACS
CSCsh68503	ISS SNMP trap: need to parse another format for ICMP type/code fields
CSCsh67287	t_semaphore class not thread safe
CSCsh60413	LC pulls data very slow when encountering DbException
CSCsh60184	4.3.1 and 5.3.1 should include the update /usr/bin/tzselect script
CSCsh58561	ADMIN > System Parameters pages have easy-to-fix heading problems
CSCsh58518	Many ADMIN sub-windows have easy-to-fix vertical alignment issue
CSCsh57236	Unknown Reporting Device was missing on GC's DB pn_device table
CSCsh57087	keyword search returned empty result for long raw messages
CSCsh56931	Rule engine fires only once if only SAME is present in any column
CSCsh56499	Mars should learn FWSM dynamic nat from syslog for sessionization
CSCsh56259	pnarchive - CF production blocked, failing silently
CSCsh55172	GC: Networks changed while LC deleted not correct after LC re-added
CSCsh54239	GC/LC pull and push servlets call CheckBoxInfo to check license every 30
CSCsh52614	Scheduler process creates extra audit log records for login
CSCsh52443	Invalid syslog message generated while upgrading through GUI
CSCsh51271	GC is unable to update LC's device name under admin/LC management
CSCsh50446	parsing error for PIX-6-113015
CSCsh49009	Duplicated GC and LC networks not displayed in fixed order on the LC

Reference Number	Description
CSCsh48988	IP groups not displayed in order
CSCsh47461	'Details' button does not return
CSCsh46958	pnparser does not clean up Oracle device map when it receives db Change
CSCsh46448	Agent list of a device not displayed in order
CSCsh46428	Available hosts list not display in order when adding agents to CSA
CSCsh46424	User group list not displayed in order
CSCsh46417	User list not displayed in order on LC
CSCsh46401	Service groups not displayed in order
CSCsh46387	Device Event IDs not displayed in order
CSCsh46183	GC - Should put up error when select details for "Non Responding" LC
CSCsh45922	archive/restore - ranged restore fails to fully preserve identity
CSCsh45564	PIX/ASA 7.2 messages 415001 to 415020 needs rewriting for parsing code
CSCsh44548	GC does not appear to update LC status
CSCsh44179	Connection Errors cause inability to select zone in incident/rule edit
CSCsh43998	system ctx for PIX/ASA 7.0 discovered as vesion 7.2
CSCsh43845	IP management GUI: User can add VA Service to a host
CSCsh42151	GUI Summary pg shows #events < #sessions & negative data reduction rate
CSCsh41594	LC is not moved from the GC after it is deleted
CSCsh40743	pink box when doing real time query and click access rule icon
CSCsh40698	VPN GroupName and Username disappeared from its raw event message
CSCsh40475	Custom GC Error display when comm to LC fails - DISA requested feature
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
CSCsh38491	Duplicate entries in 5-bigFile.txt
CSCsh36021	Need to distinguish between CSA versions on GUI
CSCsh35130	Cancel edit removes Enterasys/NS IDP Server and sensors from device list
CSCsh34170	Change/Modify report needs to purge existing reports
CSCsh32558	custom column query: for acs event log, reported user is missing
CSCsh27882	Database Client: Debug Logging leads to incomplete scheduled discovery
CSCsh27853	Report results for a 10 minute window is dropped on an 'activate
CSCsh23983	DbExportFile not working
CSCsh20677	Qualys: Discovery failed syslog from C++ backend needs to be suppressed
CSCsh20219	Confirmed user false positive query error java.lang.NullPointerException
CSCsh19644	Get browser error when select to add a new host
CSCsh18265	null drop rule causes parse error in the GUI
CSCsh14075	scheduler-service.xml.contrib present in deploy directory
CSCsh14070	CS-Mars - Microsoft Misspelled in VA section

Reference Number	Description
CSCsh13261	syslog related to upgrade through GUI sends invalid syslog messg
CSCsh13253	syslog related to upgrade server missing
CSCsh11012	Security issue with devices and logging
CSCsh06027	CS-MARS - DataBase file retrieval hyperlink uses wrong timestamp
CSCsh02908	The order of backend processes change randomly when setting log level
CSCsh02885	Cannot set GUI logging level to Trace
CSCsh02501	Query page text boxes should truncate input
CSCsh01636	JDBC update to ojdbc14.jar
CSCsh00199	Cannot add service/application to a host's vulnerability accessment info
CSCsg99611	CS-MARS - Radio buttons are confusing on Retrieve Raw Messages page
CSCsg98622	Incidents ready to fire are discarded on clicking 'Activate
CSCsg94880	GC Pink box when doing keyword search on GC
CSCsg93306	Hosts List on MARS not consistent with discovered Qualys device list
CSCsg93242	Allow customization to 15-minute session timeout setting
CSCsg93235	zone_id of Unknown Reporting Device on GC is not correct
CSCsg92417	keyword query returns incorrect number of events
CSCsg88644	recent connection in ui report is much higher than snmpwalk value
CSCsg87864	Recent average percentage for memory just is only half of actual value
CSCsg86481	CS-MARS parsing error for ASA7.0 msg 302018
CSCsg86370	FR: MARS should support CSA 5.x
CSCsg83055	parsing error for FWSM-n-302003 and FWSM-n-302004
CSCsg80661	memory percentage is over 100% in UI report
CSCsg77577	incorrect resource utilization for concurrent conn
CSCsg73843	GC - Unable to change configuration information (email IP) from GUI
CSCsg68371	cannot not use < > & to do keyword correctly
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
CSCsg64243	GC - Path Link to inactive LC in incident displays error
CSCsg60114	System error when generating NAC report
CSCsg59538	GC and LC Summary Pages - Data Reduction shows negative percentage
CSCsg53084	MARS - WebVPN ACL Parse error event fires on incorrect syslog
CSCsg49567	Admin/Retrieve Rawmsgs: some events appear twice
CSCsg44725	need to downgrade log level of CSA snmp trap errors in backend log
CSCsg44578	need to add CheckPoint NGX R61 support in MARS BOOTES release
CSCsg41549	MARS discovery issues with Loopback IP on IP Unnumbered interfaces.

Reference Number	Description
CSCsg39552	Certain FWSM 2.3 syslogs give parsing errors/unknown event type in 4.2.2
CSCsg35110	Entering a zone name with a / gives errors when importing the ssl cert
CSCsg33636	PIX/ASA version above 7.0 need to be treated the same way
CSCsg30013	windows pull watchdog sometimes restarts all MARS proc
CSCsg26225	Graphs/Images do not show up in case related report emails
CSCsg25306	CS-MARS should support EMBLEM format of syslog
CSCsg23483	device_monitor does not load device utilization history on startup
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.
CSCsg10787	CatOS telnet discovery failing.
CSCsg05143	Button functions on zone config page should be restricted
CSCsg04079	Lotus Notes client gets JavaScript error with emailed MARS report
CSCsg03167	8 unknown event type CatOS events
CSCsf30116	Event Rate on the Top Destination Port graph is not correct
CSCsf27617	pnparser enhancement - custom parser to expand three more user fields
CSCsf18192	Slow rendering of the GC/LC Summary page
CSCsf11055	CC: GUI and CLI allow different password lengths - should be same
CSCsf06819	vulnerabilities not updated for hosts reported by deleted eEye console
CSCsf02072	GC-LC communication abnormal after running long time
CSCse88764	can't access a ftp server with a user ID/password including @
CSCse84962	eEye: MARS does not remove resolved vulnerabilities from host info
CSCse84945	eEye: imported vulnerabilities that are unknown should be flagged
CSCse73788	MARS rediscovers Juniper Netscreen firewalls with wrong OS
CSCse68056	Can't chage the GUI logging Level to trace
CSCse66656	create utility to change an LC to standalone mode
CSCse60240	CS-Mars - report for old events include real-time events
CSCse57955	CS-Mars showing unknown parsing error for Netscreen 5.0 events
CSCse56430	Enhancement: Save release binaries with debug symbols for debuggability
CSCse53856	Got "Error on page" when displaying packet data from IDS device
CSCse52782	Can't change run-time to day in "Resource Issues: Server - Top Reporting
CSCse49863	the default user is not pnadmin when deleting a case owner
CSCse47519	Traffic Event is not parsing for Netscreen FW4.0 & 5.0
CSCse47244	cpu utilization value greater then 100% on a single CPU ios router
CSCse46299	Entercept Events will be unknown device event type when host OS=solaris
CSCse45018	MARS is unable to parse NetScreen 5.x syslogs
CSCse44601	java.lang.NumberFormatException : User Management screen
CSCse44345	readWebLogThread in pnparser spins if servlet socket disconnects

Reference Number	Description
CSCse40904	Save As report button not enabled.
CSCse39426	frequent superV & pnparser restarts cause log processing to fail
CSCse35420	Interface error rate should be separate from discards and unknown protos
CSCse34216	CPU utilization report numbers on UI doesn't match the SNMP query
CSCse32591	dealing with duplicate hostnames in VA import
CSCse26964	CatOS Syslog %SYS-4-P2_WARN not parsed correctly by MARS
CSCse24391	parsing error for PIX, ASA: PIX-6-607001
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
CSCse22824	CS-Mars - device_monitor: change resource not found log level to debug
CSCse21626	Clicking activate is not taking effect
CSCse20684	CSM: Test connectivity View Error message "Not Found
CSCse19198	Device Cnf: Changes in Mail Gateway IP doesn't reflect Report/ Notif
CSCse12512	Missing CSM policy query icon for events with destIP 255.255.255.255
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
CSCse03134	More control is needed over retrieve raw messages and cleanup
CSCse01877	It takes more than 2 minutes to open ip management (network) page
CSCse00417	Incorrect name for system report 'Attacks: All - Top Rules Fired
CSCsd95535	Sentence for suggested migitation cmd is incorrect (extreme)
CSCsd94152	It takes more than 5 minutes to open the schedule discover page
CSCsd92922	deleteing item in sources available list got pink box
CSCsd92285	Security Dev Edit page does not check for existing IP address conflict
CSCsd88284	optimizing incident inserts in DbIncidentLoaderSrv
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
CSCsd53173	Retrieve raw messages doesn't properly update the progress percentage
CSCsd48097	Event processing may stop if pnparser creates shared buffers first
CSCsd45441	unknown reporting IP: 127.0.0.1 from checkpoint
CSCsd37005	user must be able to change own password
CSCsd28382	error in data work for event type 6000512 : "Virus - Possible pif Worm
CSCsd22832	Attempt to remove IP subnet from IP Management fails, with error

Reference Number	Description
CSCsd20196	User and System Scheduled Reports fail to display data
CSCsc73832	Drop rule inactive for events received by netflow in CS-MARS
CSCsc70982	change the button string on the false/positive column to "Tune
CSCsc70832	SNMP Device Discovery should identify ASA device
CSCsc66267	Oracle User name in the reported user field of MARS
CSCsc58485	5 tuple information missing from downloaded raw log file
CSCsc32363	Documentation request GC LC communication troubleshooting
CSCsc30107	Cs-Mars - Queries with != in service column don't work
CSCsc26340	'occured' misspelled in MARS e-mail alerts
CSCsc24955	ISS Site Protector central server log's are not supported by MARS
CSCsc10453	Show resolved host name in report if device was not found in system
CSCsc07377	Dynamic Info page on mitigation shows ip addess as -1.-1.-1.-1
CSCsc02847	Rule disappears from its group after edited in its Inactive status
CSCsc01793	GUI logging levels is not changed correctly
CSCsb60747	Ciscoization - GC zone models aren't Cisco-ized
CSCsb57624	Unknown report device in Checkpoint log
CSCsb55704	LC Certificate Mis-placed in GC after a new LC added
CSCsb44374	FWSM's access was not displayed on the security info page
CSCsb43627	Source IP address is not correct for a VPN3K event
CSCsb39208	Unrecognized Traps from McAfee EPO
CSCpn03077	GC, sys error when adding a LC which was added to GC already
CSCpn03053	GUI log level setting is not working as expected
CSCpn03005	Loading Resource Util report as On-Demand query produces a system error
CSCpn02930	Error message when adding non-existent LC to GC is incorrect
CSCpn02892	Licensing: Inputting valid LC license onto GC allows the user to run
CSCpn02693	6MB mem leak in process_event_srv after each activate
CSCpn02590	In summary page, data reduction shows 100% when it should be 0%
CSCpn01934	Back button is missing in logging level/log/audit trail pages
CSCpn01465	Reports: have "View", "Add" etc. buttons at top of page
CSCpn01317	More data expected when populating pn_application table
CSCpn01293	Host OS listing needs cleaning
CSCpn00887	Summary: Inconsistent title bar naming convention for the Summary Pa
CSCpn00845	Editing service to become ICMP w/o ICMP code -> no change

Resolved Caveats - Releases Prior to 5.3.1

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