Release Notes for Cisco Security MARS Appliance 5.3.5

Revised: June 10, 2008, OL-16728-01

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

Introduction

Version 5.3.5 is now available as an upgrade of 5.3.4 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 5.3.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.

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

Registered SMARTnet users under the can obtain version 5.3.5 from the Cisco support website at:

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

Supported Hardware

Cisco Security MARS Version 5.3.5 supports the following Cisco Security MARS Appliance models:

Local Controller Appliances

- Cisco Security MARS 25R (CS-MARS-25R-K9)
- Cisco Security MARS 25 (CS-MARS-25-K9)
- Cisco Security MARS 55 (CS-MARS-55-K9)
- 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:

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

Miscellaneous Changes and Enhancements

The following changes and enhancements exist in 5.3.5:

- **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 2
- **Bug fixes.** For the list of resolved issues, see Resolved Caveats - Release 5.3.5, page 16.

New Vendor Signatures

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

Revised in 5.3.5	Product	Signature Version Supported
Intrusion Prevention and Detection Signatures		
Yes	Cisco IDS 4.0, Cisco IPS 5.x, Cisco IOS 12.2	Current through S330 signature release.
Yes	Snort NIDS 2.6.1	Current through the April 8, 2008 signature release. Latest signature mapped: 13664.
Yes	ISS RealSecure Network Sensor 6.5 and 7.0, and ISS RealSecure Server Sensor 6.5 and 7.0	XPU 28.050 Release date: April 8, 2008
Yes	McAfee IntruShield NIDS 1.5 and 1.8 McAfee Network Intruvert v. 2.5, 4.0	4.1.24.5 Release date: April 7, 2008
Yes	McAfee Entercept HIDS 2.5, 4.0	Current through the April 11, 2008 signature release.
Yes	CheckPoint Application Intelligence (VPN-1 NG with Application Intelligence R55)	Current through the April 8, 2008 signature release
Yes	Netscreen IDP 2.1, 3.0, 3.1, 4.0, 4.1	Signature version: 4.1. Release date: April 10, 2008
Yes	Symantec NIDS, v 4.0	Signature package: 95 Release date: April 11, 2008
Yes	Enterasys Dragon 6.x, 7.x	Current through the April 10, 2008 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.
Vulnerability Scanner Signatures		
Yes	Qualys QualysGuard ANY	Current through the April 11, 2008 signature release.
Yes	E-Eye, Retina Scanner Vulnerability Software, version 5.6[1]	Current through the April 10, 2008 signature release.
Yes	Foundstone, version 3.x	Current through the April 15, 2008 signature release.
Yes	Common Vulnerabilities and Exposures (CVE) Database	Current with the April 17, 2008 definition update.
Miscellaneous Support		
No	Oracle 11g	Support for new AUDIT_ACTIONS.

1. eEye REM 1.0 is supported in 4.2.x.

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.

General Notes

The MARS Appliance performs a file system consistency check (fsck) on all disks when either of the following conditions is met:

- If the system has not been rebooted during the past 180 days.
- If the system has been rebooted 30 times.

The fsck operation takes a long time to complete, which can result in significant unplanned downtime when rebooting the system after meeting a condition above. For example, a MARS 50 appliance can take up to 90 minutes to perform the operation.

Upgrade to 5.3.5

No important notes exist for the 5.3.5 upgrade.

Upgrade to 5.3.4

No important notes exist for the 5.3.4 upgrade.

In addressing *CSCsm57453: Incident not created for some of same events*, the behavior now differs between 4.3.4 and 5.3.4. In the x.3.3 releases, incident firing was throttled at 100 incidents for event bursts from a vulnerability assessment (VA) reporting device. In 5.3.4, incidents firing throttles at over 430 incidents, and in 4.3.4, the incidents firing throttles at just over 220 incidents.

Upgrade to 5.3.3

No important notes exist for the 5.3.3 upgrade.

Upgrade to 5.3.2

The upgrade is from 5.3.1 to 5.3.2. The following important notes exist for this upgrade:

- **Release-Note for CSCsk19730/CSCsk12130**

  If you've edited a system rule on a Global Controller, you may enounter one of two conditions where the rules on the Global Controller are out of sync with those on the Local Controller.

  Symptom: The edited rule in the Global Controller disappears from the list of rules on the Local Controller. (CSCsk12130)

  Condition: The user edited a rule on the Global Controller and then upgraded to a different version of the MARS system software and then added of a new Local Controller to the Global Controller.

Symptom: A rule that was edited in the Global Controller looks as if it is an empty rule in the Local Controller and be inactive. (CSCsk19730)

Condition: This occurs under in some cases where a Local Controller is added to a newly upgraded Global Controller.

Work Arounds: If the Local Controller is deleted from and re-added to the Global Controller under x.3.2, the issue should resolve itself. However, in conditions with a large topology or many custom rules, we recommend contacting technical support for a work around that avoids the need to delete and re-add the Local Controller.

Another possible work around if the number of edited rules are small is to edit and make further changes to the rule and activate. In this case, the issue should be resolved for that rule.

- **Upgrade of IOS 12.3 and 12.4 devices.** In previous releases, these devices were supported under the IOS 12.2 release when defining the device type in theMARS web interface. After you upgrade to 5.3.2, the next discovery of such a device will automatically upgrade the version to its correct value.

  For example, an IOS 12.4 device is added to MARS 5.3.1 as 12.2 and after the upgrade to 5.3.2, when the discovery occurs for that device, the device type is automatically updated to IOS 12.4. The same is true for devices that are running IOS 12.3. However, if you have not enabled device discovery, use the Change Version feature to change between IOS 12.2, 12.3, and 12.4.
- **Wireless LAN Controller Support is restricted to the 5.3.x train.** To enable support for wireless access points via the Cisco Wireless LAN Controller, you must use the 5.3.2 or later software, which also restricts the appliance models that can be used.
- **Juniper/NetScreen IDP 3.x and 4.x Support is incomplete.** While device support has been added, the signature/data work portion of these devices will be provided in a future release of MARS software.
- **Renaming of QualysGuard 3.x device type.** During the upgrade, any QualysGuard devices defined under Security and Monitoring Devices will changed their device type from QualysGuard 3.x to QualysGuard ANY.

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.

5.3.

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
5.3.1	5.3.2	csmars-5.3.2.pkg
5.3.2	5.3.3	csmars-5.3.3.pkg
5.3.3	5.3.4	csmars-5.3.4.pkg

Documentation Errata

- CSCsl14244. User guide does not discuss role of Nessus in the MARS system.

  To determine whether specific incidents are false positives, MARS uses Nessus 2.x GPL plug-ins and custom scripts mapped to specific MARS event types. MARS does not use Nessus to perform vulnerability assessments or related reporting.

- CSCsk77546. Discovery Device with SSH 512 module not supported.

  The OpenSSH client used by MARS does not support modulus sizes smaller than 768. For example, you cannot discover a device using a SSH login that has 512-byte key.

- CSCso30490: CS-MARS: RAW Message Retrieval to NFS server doesn't work

  In 5.3.4, you must manually define a cache folder on your NFS server before you can retrieve raw messages from an NFS archive. This cache folder must adhere to following guidelines:

  – Create a folder named **/tmp/MARSCache** on the same NFS server as the archive is to be stored. For example, if the archive is configured to write to 10.1.1.1, create a /tmp/MARSCache folder on that 10.1.1.1 host.

  – The /tmp/MARSCache folder is absolute path; **/tmp** must be at the same level as root.

  – The /tmp/MARSCache folder should be unique on the NFS. Do not use this path for the value of the Archival field. The Archival field cannot have a value of /tmp/MARSCache.

  - The MARS appliance should have write permission to the /tmp/MARSCache folder on NFS server.
  - MARS does not clean up the /tmp/MARSCache folder.
  - Ensure that sufficient disk space on the NFS server is allocated to this cache.

Important Notes

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

- If the client system used to access the MARS GUI is not on the same side of the NAT boundary as the a MARS appliance and the Security Manager server, you can perform policy lookup in read-only mode. However, you cannot start the Security Manager client from the read-only policy lookup table to modify matching policies. The client system must be on the same side of the NAT as the MARS appliance and the Security Manager if you want to the Security Manager client from MARS to modify the matching policy.
- Security Manager client must be on the same side of the NAT boundary as the MARS appliance and the Security Manager server to query MARS events from policies.
- 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.
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 5.3.5, page 9
- Resolved Caveats - Release 5.3.5, page 16
- Resolved Caveats - Releases Prior to 5.3.5, page 16

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 5.3.5

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

Reference Number	Description
Cisco Security Manager	
CSCso16735	xCSM: P->E with CS Mgr credentials fails in cross-launched CSM client
CSCsm94630	Policy query icon is not shown at times in Real time viewer
CSCso11900	Keyword field dimmed in Query page after events lookup from Security Mgr
CSCsm96376	Policy lookup icon not shown if device is deleted from MARS
CSCsm14585	Read-only policy page takes a long time to display for realtime events
CSCsm92008	Security Manager not reachable error displayed after long time
CSCsm94537	Policy lookup icon not shown for a device deleted and readded to MARS
CSCsl54107	Security Manager policy lookup for ICMP connection teardown syslog fails
CSCsm43237	Minimum password length for Security Manager account in MARS
CSCsf31401	MARS query does not highlight rules inside any policy group named Local
Firewall Services Module	
CSCsl27574	FWSM Syslog message FWSM-6-302013 with wrong Real and Mapped IP

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

Reference Number	Description
CSCsq69190	4.3.5 eth1 IP address not migrated to 5.3.5
CSCsq33307	Custom device still shows up in the device list even after deleting it
CSCsq33040	On LC seeing pn_statistics_data with zone set to 0 (sometimes)
CSCsq29469	MARS: Detailed NAC report with keyword query has empty columns
CSCsq23660	Telnet to port 22 returns SSH Banner
CSCsq23060	Entries with ID 0 exist in database in some tables
CSCsq15630	Confirmed false positive did not show in GUI
CSCsq07542	CS-MARS Incident path graph connects to wrong cloud/gateway
CSCsq05336	MARS - Large Number of Reported Users, Query user selection fails
CSCsq01029	MARS Gen1 - Need Message Pointing to Failed Drive for Replacement
CSCso97681	Host name appears inconsistently on Incident Vector Topology
CSCso93030	IP Management not displaying group associations when using Device Group
CSCso89940	MARS: User-Name in raw message not populating user column in NAC report
CSCso87624	MARS IOS Discovery failure when banner has number/pound (#) symbols
CSCso86201	Vulnerabilities found against MARS unit
CSCso80923	Specific Patter From a Customer Parser is Not Synced to LC
CSCso80816	Dashboard to report relations fail to replicate LC/GC
CSCso73998	Editing User Group From Rules/Action Menu Clears Group Members
CSCso72148	Host name Any can be added via VA scan report in MARS
CSCso70178	shared buffer does not update write_stop_time correctly
CSCso62981	Gen 2: Raw Message Retrieve doesn't work due to different time zone used
CSCso61036	LC/GC Sync: Improve handling of config pull on update
CSCso60384	TR/RR not present in results for All Matching Events - LLV raw events
CSCso59056	pnrestore throws the warning of archive version 0
CSCso54308	LC stops communincating to GC, stack dump shows stuck in Version Check
CSCso53066	DbInterface's interface_index value's precision has to be 10
CSCso50724	pnparser memory leak in parsing error handling caused restart by superV
CSCso43238	LC pull of updated GC rule fails if rule has been edited at LC
CSCso40549	L2 path through 7600 with VRF give error message
CSCso39840	Sud incr. in traf raw msg should have std deviation instead of variance
CSCso38232	Host not shown in topology graph if Security Manager is added on it
CSCso32099	Some ISS events parsing error on MARS
CSCso28421	AAA: When adding AAA server cannot select existing ACS
CSCso27861	Sym Agent load thru seed file returns ArrayIndexOutOfBoundException
CSCso09952	MARS shows unknown reporting IP:0.0.0.0 for events from WL controller

Reference Number	Description
CSCso01260	Loading hosts from seed file does not fill interface information on MARS
CSCsm95233	host appears in edit, but not view of group
CSCsm92836	Large interface index causes SQL errors during DB save of interfaces
CSCsm81377	Mars 4.3 - not able to set custom POSIX timezone opt 11
CSCsm75403	Network groups ignored in query
CSCsm60645	MARS dropping some events
CSCsm56006	PIX|ASA70 - Event parsing errors
CSCsm55954	detailed NAC report table header does not show in the schedule report
CSCsm55938	PIX|ASA: Event parsing errors
CSCsm48603	config change report didn't capture cat6k/vpn3k config change events
CSCsm45118	CSA Events in MARS appear as hex characters
CSCsm40349	rare crashing issue due to file system check/memory short
CSCsm38062	MARS change wrong device type when use SNMP as access type
CSCsm28714	Need CLI/UI method for retrieving log files
CSCsm09021	Wrong query interval if leave one field blank
CSCsm09020	"missing_zone_info" incidents show up in the GC
CSCsl77531	Device monitor uses excessive memory, repeatedly restarted by superV
CSCsl58359	exporting data use pnexp requires more TEMP tablespace
CSCsl58216	MARS Layer 2 path and mitigation issues with IOS 12.3 and 12.4 version
CSCsl41494	Network_group object with DB ID of 0 (zero) causes system error in GUI
CSCsl31143	MARS restore process fails on 4.3.1
CSCsl14244	The User guide is not talking anything about the Nessus version
CSCsl11647	Pnupgrade hanging at the last step - Updating database schema
CSCsl04692	Reported user is not parsed for windows event id: 680
CSCsk92543	CS-MARS: Custom Column Report Device Column Blank .
CSCsk85267	pnparser crashes related to CheckPoint Opsec library
CSCsk85174	MARS - 5 tuple information missing from raw IDS events from NFS archive
CSCsk80647	pnupgrade is not displaying next fsck scenario
CSCsk70744	Upgrade OpenSSL version
CSCsk39645	GUI doesn't check duplicate agent ip address when adding application
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
CSCsk12489	operator role can not resubmit report
CSCsk12421	Netflow config wrongly mixed up with traffic anomaly configuration
CSCsk11592	ids didn't get monitored networks from msfc if discover ids first
CSCsk08028	Real time multi column query is not working.

Reference Number	Description
CSCsk04282	MARS failed to import 1000 hosts vulnerablilty information
CSCsj96592	Adding LC with version lower than 4.3.1 should version mismatch err
CSCsj92673	pink box appears when adding query/Report into Cases
CSCsj90875	Inline/Batch query: result mismatch on Matched Rule Ranking
CSCsj90505	Inline/Batch query not match on NAT connection report
CSCsj87207	GUI cannot show the full topology because of constant process crash
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
CSCsj60272	Special characters should not be allowed in device name(MARS)
CSCsj51240	Paging does not work for report right after adding it to a case.
CSCsj42467	LC not showing up on certificate page
CSCsj31990	pnparser: to avoid flooding log file
CSCsj28376	Box may not be able to reboot after recovery, under certain conditions
CSCsj23845	CS-MARS Action filter doesn't work if 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
CSCsi96921	IPSDynamicSigUpdate attempts to connect to CCO with no credentials
CSCsi93283	Mismatch between query and report results for source port ranking.
CSCsi91734	Mismatch in results between query and report for All Matching Events
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.
CSCsi65960	L2 mitigation has problem finding path
CSCsi65713	Index needs to be removed for the pn_report_result table
CSCsi62384	The performace test kills all the process during the weekend run
CSCsi52731	mars reboots w/o asking for confirmation after user clicked cfg update
CSCsi51999	Edit SW based Application device need submit twice
CSCsi50024	IPS is not visible in Global Zone Hot Spot 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.

Reference Number	Description
CSCsi44427	Enh: Make HTML report output the same as CSV output
CSCsi29398	CS-Mars does mitigate to the proper endpoint
CSCsi18757	CS-MARS - Request to have the "ssldump" command in the MARS CLI.
CSCsi15769	NLS_LANG variable should be updated in environment
CSCsi13100	gui.sh dev build makes different JBOSS web.xml than make release
CSCsi11312	pn_incident_log and pn_report_log should be archived
CSCsi07186	User can input unsupported characters in AAA device name
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.
CSCsh89445	GUI allow users create rule without putting rule name
CSCsh83068	Report and query return no results under device type ANY
CSCsh73553	MARS DVD imaging does not support USB keyboard
CSCsh67828	Custom Column Query filtered by reporting device missing results
CSCsh52537	Repeated upgrades of oracle fills hard drive
CSCsh44351	CSM multiple hostname matches failed to return multiple hosts
CSCsh14454	server.log can grow unbounded with in a single day
CSCsh00013	Case Management: history does indicate change of ownership
CSCsg91816	port 0 in 'Top Destination Ports' misleading
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
CSCsg73786	Devices should not be added to MARS if Discovery is unsuccessful
CSCsg64119	rule's keyword editor treats NOT as binary rather than unary
CSCsg54313	ORA-01654: unable to extend index .
CSCsg47022	CS-MARS - Incorrect Start Times on Retrieved Raw Message Files
CSCsg26352	Getting a internal server error when trying to access a incident on GC
CSCsg20987	CSMARS DTM sdf files are sent with invalid format
CSCsf99844	wrong values for current connections using CLI "show resource usage
CSCsf99767	provide encoding selection for adding agent to device/host
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

Reference Number	Description
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
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)
CSCse82042	Change the Device Type Version for FWSM
CSCse82022	Unable to view reports starting with #sign in csv format
CSCse78738	FWSM ifspeed incorrectly reported as 0 for per-context vlan interfaces
CSCse78089	Unable to upgrade CS-Mars via GUI
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%
CSCse44509	On demand report progress shows negative value
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
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
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
CSCse00626	IP Management -> device group displays hosts only.
CSCsd95582	Both successful/failed mitigation reports show same results
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
CSCsd61749	pnrestore doesn't restore all of the system config
CSCsd06302	device name with single quote causes pink box
CSCsc95831	log messages of MARS processes stopped being written into backend log

Reference Number	Description
CSCsc90480	MARS Incident notification options are not configurable
CSCsc59363	Need improvement to GUI for multi-line rules
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
CSCpn02869	Rules editing: changing entry for select window pulldown after error
CSCpn02804	Replay History feature not working correctly
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
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

Reference Number	Description
CSCpn01134	Cloud name input box accepts invalid characters
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

Resolved Caveats - Release 5.3.5

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

Reference Number	Description
CSCsq68939	adding gen-1 LC to a gen-2 GC runs into error
CSCsq56260	unable to login to installed 5.3.5 2930 GC from GUI.
CSCsq45773	Data upgrade not happening from 5.3.4 to 5.3.5 using package
CSCsq30468	x.3.5 packages have different IPS signature levels
CSCsq23405	LC/GC Configuration Pull causes unnecessary Activation
CSCso69721	Mars 4.3 - Some IPS events showing up with no event type
CSCso67351	CS-MARS: IPS Sig 5733 Maps to "WWW IIS Internet Printing Overflow" event
CSCso45101	ASA 8.0.3 : Parsing Errors for some messages
CSCso02939	Replace IPS signature link
CSCsm98909	MARS - Firewall Syslog ID 111008 Event Type name is misleading
CSCsm93557	LC/GC Not replicating large report result sets > 1000 elements
CSCsm79939	IP address in "More info of this device " is incorrect for Netscreen 5.0
CSCsk02989	GC is not usable when LC has lots of deleted devices
CSCsc97963	Netscreen logical interfaces (vlan intf) not discovered

Resolved Caveats - Releases Prior to 5.3.5

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