# Release Notes for Cisco Security MARS Appliance 6.0.3

**Published: April 6, 2009**
**Revised Date:July 24, 2009**

**Note** We sometimes update the printed and electronic documentation after original publication. Therefore, you should 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), Release 6.0.3 running on any supported MARS Appliance model listed in Supported Hardware, page 2.

This chapter contains the following topics:



# Introduction

Release 6.0.3 is now available as an upgrade of 6.0.2 of your software release in support of the MARS Appliance models as identified in Supported Hardware, page 2. Registered SMARTnet users can obtain release 6.0.3 from the Cisco support website at:

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

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

And then click the **Download Software** link in the Support box on the right side of the MARS product home page.

# Supported Hardware

Release 6.0.3 supports the following Cisco Security MARS Appliance models:

**Local Controller Appliances: 2nd** Generation

- 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)

**Local Controller Appliances: 1st** Generation

- Cisco Security MARS 20R (CS-MARS-20R-K9) as a MARS 20
- Cisco Security MARS 20 (CS-MARS-20-K9)
- Cisco Security MARS 50 (CS-MARS-50-K9)
- Cisco Security MARS 100e (CS-MARS-100E-K9) as a MARS 100
- Cisco Security MARS 100 (CS-MARS-100-K9)
- Cisco Security MARS 200 (CS-MARS-200-K9)

**Global Controller Appliances: 2nd** Generation

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

**Global Controller Appliances: 1st** Generation

- Cisco Security MARS GCR (CS-MARS-GCR-K9) as a MARS GC
- Cisco Security MARS GC (CS-MARS-GC-K9)

# New Features

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

This section contains the following topics:



## Miscellaneous Changes and Enhancements

The following changes and enhancements exist in :

- **Credential Automation**—Save administrative time by updating many Cisco device credentials in a single operation rather than touching each device definition in MARS. Using a seed file to re-import devices that are already defined in MARS, users can update some credentials for Cisco ASA, Cisco PIX, Cisco IPS, Cisco IOS, and Cisco Switch devices.
- **Actionable Incident Notification—**This enhancement helps customers decide on the importance of a notification without having to log into MARS. The MARS syslog, e-mail, and SNMP incident notification messages provide incident summary information as well as Top 3 reports. The incident summary will include the rule ID, rule name, incident ID, incident start/end time and incident severity. Top 3 reports include Top 3 destination ports, Top 3 reporting devices, and Top 3 event types.
- **Improved Reporting Response Times**—This enhancement improves response times of commonly used reports by retrieving event data from memory rather than from the database.
- **Exported/Archived Configuration Validation**— This enhancement ensures that you do not attempt to restore or upgrade a system using a corrupted configuration file. After exporting or archiving a configuration file, MARS scans the file to make sure it is not corrupted.

# New Device Support

The 6.0.3 release of MARS supports the following new device versions:

- Cisco IPS 6.2 (backward compatible mode)

# New Vendor Signatures

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

**Tip** For full details on supported devices and versions, see Supported and Interoperable Devices and Software for Cisco Security MARS Local Controller 6.0.x.

| Revised in 6.0.3 | Product | Signature Version Supported |
|---|---|---|
| **Intrusion Prevention and Detection Signatures** | | |
| Yes | Cisco IDS 4.0,<br>Cisco IPS 5.x,<br>Cisco IPS 6.x<br>Cisco IOS 12.2 | Current through S382 signature release. |
| Yes | Snort NIDS 2.8 | Current through the February 3, 2009 signature release.<br>Latest signature mapped: 15294. |
| Yes | ISS RealSecure Network Sensor 6.5 and 7.0, and<br>ISS RealSecure Server Sensor 6.5 and 7.0 | XPU 29.020<br>Release date: February 10, 2009 |
| Yes | McAfee IntruShield 4.1 | v4.1.41.8<br>Release date: January 13, 2009 |
| Yes | McAfee Entercept HIDS 2.5, 4.0, 6.x | Current through the January 23, 2009 signature release. |

| Revised in 6.0.3 | Product | Signature Version Supported |
|---|---|---|
| Yes | CheckPoint Application Intelligence (VPN-1 NG with Application Intelligence R65) | Current through the February 2, 2009 signature release. |
| Yes | Netscreen IDP 2.1, 3.0, 3.1, 4.0, 4.1 | Signature version: 4.1.<br>Release date: February 10, 2009 |
| No. EOS. | Symantec NIDS, v 4.0 | Signature package: 95<br>Release date: June 12, 2008 |
| Yes | Enterasys Dragon 6.x, 7.x | Current through the February 10, 2009 signature release. |
| No. EOS. | Symantec Manhunt 3.x<br>(See Symantec NIDS, v 4.0.) 3.4.3 Update 59 | 3.4.3 Update 59<br>Current through the May 24, 2007 signature release. |
| **Vulnerability Scanner Signatures** | | |
| Yes | Qualys Guard ANY | Current through the February 10, 2009 signature release. |
| Yes | E-Eye, Retina Scanner Vulnerability Software, version 5.6[New Vendor Signatures, page 3] | Current through the December 12, 2008 signature release. |
| Yes | Foundstone, version ANY | Current through the February 9, 2009 signature release. |
| Yes | Common Vulnerabilities and Exposures (CVE) Database | Current with the February 9, 2009 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 upgrades. In addition to addressing high-priority caveats, 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 *Cisco Security MARS Initial Configuration and Upgrade Guide*.

## Important Upgrade Notes

To ensure that the upgrade from earlier releases 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 6.0.3

No important notes exist for the 6.0.3 upgrade

## Upgrade to 6.0.2

No important notes exist for the 6.0.2 upgrade

## Upgrade to 6.0.1

The upgrade process to 6.0.1 differs based on the release you are upgrading from. If you are upgrading a 5.x release, then you can upgrade to 6.0.1 if you are running 5.3.6. The upgrade from 5.3.6 to 6.0.1 takes several hours, as it also upgrades the Oracle database running on the appliance. If you are running an earlier 5.x release, you must first upgrade to 5.3.6 (see Upgrade to 5.3.6, page 5 for details).

However, if you are upgrading a 4.x release, you must migrate the system instead of upgrading. To migrate from a 4.x, you must follow the step-by-step instructions specified in the Migrating Data from Cisco Security MARS 4.x to 6.0.1.

**Note** When upgrading a "restricted" model of MARS appliance (20R, 100e, or GCm) to MARS Software release 6.0.1, all limits enforced by the restricted model will be ignored. The "restricted" models will perform as unrestricted models (20, 100, or GC) once upgraded to release 6.0.1.

## Upgrade to 5.3.6

For notes that are specific to the upgrade to the 5.3.6 release, as well as all previous 5.x releases, see the Release Notes for Cisco Security MARS Appliance 5.3.6.

## Upgrade to 4.3.6

For notes that are specific to the upgrade to the 4.3.6 release, as well as all previous 4.x releases, see the Release Notes for Cisco Security MARS Appliance 4.3.6.

# Upgrade Path Matrix

When upgrading from one software release to another, a prerequisite release is always required. This prerequisite release is the minimum level required to be running on the appliance before you can upgrade to the most recent release. Table 1 on page 6 identifies the upgrade path that you must follow to reach the minimum level required to upgrade to current release.

***Table 1 Upgrade Path Matrix***

| From Release | Upgrade To | Upgrade Package |
|---|---|---|
| 4.3.6 | 6.0.1 | *Migration required*. See Migrating Data from Cisco Security MARS 4.x to 6.0.1 |
| 5.3.6 | 6.0.1 | csmars-6.0.1.3066.pkg |
| 6.0.1 (3066) or 6.0.1 (3070) | 6.0.2 | csmars-6.0.2.3102.zip |
| 6.0.2 | 6.0.3 | csmars-6.0.3.3188.zip |

# Downloading the Upgrade Package from CCO

Upgrade images and supporting software are found on the CCO software download pages dedicated to MARS. You can access these pages at the following URLs, assuming you have a valid CCO account and that you have registered your SMARTnet contract number for your MARS Appliance.

**Top-level page:**

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

And then click the **Download Software** link in the Support box on the right side of the MARS product home page.

*Result*; The Download Software page loads.

From this top-level page, you can select one of the following options:

- CS-MARS IPS Signature Updates Archives
- CS-MARS IPS Signature Updates
- CS-MARS Patches and Utilities (supplementary files)
- CS-MARS Recovery Software
- CS-MARS Upgrade Packages

**Note** If you are upgrading from a release earlier than those posted on CCO, please contact Cisco support for information on obtaining the required images. Do not attempt to skip releases along the upgrade path.

For information on obtaining a CCO account, see the following URL:

- http://www.cisco.com/en/US/applicat/cdcrgstr/applications_overview.html

# 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.

  MARS uses Nessus as one component in determining false positives. When a host resides on a network listed under "Networks for Dynamic Vulnerability Scanning", then MARS uses Nessus to help ascertain whether an attack targeting that host was likely to be successful. When an event does not have corresponding Nessus Attack Scripting Language (NASL) script, MARS uses nmap OS fingerprinting to determine the destination operating system type, and uses nmap-found-OS to match known operating systems affected by the attack.
- 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.

# Important Notes

The following notes apply to the MARS 6.0.x releases:

- CSCsu50839—Report Result Page saves the previous "Other views" selection

  If you change the "Other Views" options in the report result page, the changes persist for that report and for that browser. When the report results are viewed later, the browser shows the saved options but the results displayed are always the default options results.

  To avoid this issue, always click **Display Report** to view a scheduled report's results.
- 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 Security Manager client must be on the same side of the NAT as the MARS appliance and the Security Manager server if you want to modify the matching policy from MARS. This restriction is also true if you want to query MARS events from policies.
- 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 in Release x.3.4 through 6.0.1. 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.interface. For
- 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*: Back-end IPS process runs at 99% CPU when pulling large IP Logs The Back-end IPS process reaches 1GB in memory used when pulling IP Logs. The process names depending on the version on MARS that is running:<br>• In release 4.2.1 and earlier, the process names are pnids50_srv and pnids40_srv.<br>• In release 4.2.2 and later, the process is named csips.<br>These related issues, are specific to pulling IP logs from Cisco IDS/ IPS devices. The symptom is that the Back-end 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.<br>*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:<br>• 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.<br>• 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.<br>*Workaround*: Refresh the page before clicking a renamed cloud. |
| CSCpn01270 | *Issue*: The free-form search may not work for the following devices:<br>• Check Point Opsec NG FP3<br>• Cisco CSA, 4.0<br>• Cisco, IDS, 3.1 and 4.0<br>• ISS, RealSecure, 6.5 and 7.0<br>• Entercept Entercept, 2.5 and 4.0<br>• 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.<br>*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.

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

This section contains the following topics:



## Open Caveats for Supporting Devices

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

| Reference Number | Description |
|---|---|
| **Cisco Security Manager** | |
| CSCsm96376 | Policy lookup icon not shown if device is deleted from MARS |
| CSCsm94537 | Policy lookup icon not shown for a device deleted and re-added to MARS |
| 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 |

## Open Caveats— Release 6.0.3

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

| Reference Number | Description |
|---|---|
| CSCpn00173 | Nessus should check pre-NAT address instead of Post-NAT address |

| Reference Number | Description |
|---|---|
| CSCpn00183 | Adding devices w/o "Activate" can cause "messy" graph |
| CSCpn00212 | Graphgen crashes when there are many non-existent devices |
| CSCpn00293 | using TAB in editing fields |
| CSCpn00455 | Graph doesn't refresh when a cloud is renamed |
| CSCpn00586 | nasl message text needs to be changed |
| CSCpn00908 | "Domain" in Configuration page - no use |
| CSCpn01134 | Cloud name input box accepts invalid characters |
| CSCpn01219 | Cleanup script for invalid /etc/qpage.conf entries |
| CSCpn01293 | Host OS listing needs cleaning |
| CSCpn01319 | pnreset command does not cause reboot |
| CSCpn01382 | Security device type hosts don't show up in IP management |
| CSCpn01398 | Unable to shutdown an interface |
| CSCpn01438 | Batch Query: Under high load, some batch queries may not complete |
| CSCpn02061 | Saving .csv files under WinXP SP2 results in .htm extension |
| CSCpn02177 | Docs: Filesystem Check after 22 reboots |
| CSCpn02251 | License: Upon entry of 100 license onto 100e, need to restart pnpars |
| CSCpn02383 | IIS parsing must be separated from Windows log |
| CSCpn02385 | Applied $TARGET01 for GC Query Source IP resulted in "resultCounter |
| CSCpn02398 | XML escaping errors in Keyword Search in Rule |
| CSCpn02410 | rule was not fired because Oracle log used upper case for user |
| CSCpn02414 | GC/LC user rule is too long to fit into a page if keyword is long |
| CSCpn02470 | Server csv function could not handle special characters in password |
| CSCpn02511 | need to fix errors in affected os |
| CSCpn02549 | JavaScript Error from ViewReport when clicking Edit/Clear |
| CSCpn02558 | "Agent" didn't be removed correctly |
| CSCpn02566 | rebooting mars while it is upgrading cause the box not accessible |
| CSCpn02574 | Time change on system causes GC/LC communication problem |
| CSCpn02653 | No way to specify "!Keyword" without a good "keyword" |
| CSCpn02666 | Batch Query Results with one item returned -> no data in graph in em |
| CSCpn02869 | Rules editing: changing entry for select window pulldown after error |
| CSCpn02901 | GC/LC, rule does not display user <cxu> but allows such cfg |
| CSCpn02968 | Network group search is not working for "All IP addresses" |
| CSCpn02973 | Not able to downgrade a security analyst to Notification only user |
| CSCpn02976 | GC:LC - Communication issues after time zone change |
| CSCpn03057 | Copied rules have shortened year in front, which is confusing (ex. 0 |
| CSCsb67871 | Got System Error In GC After Re-installed New Version In LC |
| CSCsb77550 | CSV-re import of CSA and Symantec agents unsuccessful |

| Reference Number | Description |
|---|---|
| CSCsb80082 | Deleting a LC w/o exchanging certificates doesn't set mode to Standalone |
| CSCsc04484 | LC Rule/Report list shows empty after deletion of GC group |
| CSCsc59363 | Need improvement to GUI for multi-line rules |
| CSCsc90480 | MARS Incident notification options are not configurable |
| CSCsd06302 | device name with single quote causes pink box |
| CSCsd61749 | pnrestore doesn't restore all of the system config |
| CSCsd84350 | CS-MARS/CSM: Credentials change on CSM side not checked. |
| CSCsd86896 | Clicking the clear button when editing the query type doesn't work. |
| CSCsd89457 | Incorrect handling of time range for rules that fire periodically. |
| CSCsd95582 | Both successful/failed mitigation reports show same results |
| CSCse09127 | Failed load from csv returns incorrect status |
| CSCse10945 | Summary Page Graphs Spontaneously Change Displayed Size (w/ multi-head) |
| CSCse17936 | 5K Lines Custom Query fails |
| CSCse18816 | UI takes 99% CPU, hanging browser and slowing system while expanding all |
| CSCse31722 | Cloud toggle only works on first page of reporting devices |
| CSCse33172 | Invalid id used in DbClient::retrieve() 0 |
| CSCse34407 | Query Tab -> Multi column query returns wrong results. |
| CSCse34600 | configurable SNMP timeout support |
| CSCse42953 | CS-Mars - unable to show L2 path when source and destination in same net |
| CSCse45884 | LLV query causes client CPU to go to 100% |
| CSCse51642 | IPlanet Unknown Device Event Type Parsing Error |
| CSCse54808 | The time stamp shown by the pndbusage command is incorrect. |
| CSCse85972 | Unresolved symbol in Java build (though didnot stop building) |
| CSCse98029 | Occasionally corrupted event data enters into MARS database |
| CSCsf11651 | Device resource monitor incorrectly samples 5 sec CPU instead of 5 min |
| CSCsf12825 | GUI should prevent edit/delete of system-context PIX/ASA 7.0 devices |
| CSCsf15781 | Database table columns do not match with the archive file columns |
| CSCsf26715 | Inaccuracy in per-context memory utilization for multi-context devices |
| CSCsf27568 | keyword search query can't display big-5 encoding raw msg |
| CSCsf31207 | Mars doesn't support new/changed FWSM 3.1.3 maintenance release syslogs |
| CSCsf31228 | Unknown device events for FWSM 3.1 FWSM-3-717001 till FWSM-4-717031 |
| CSCsf99767 | provide encoding selection for adding agent to device/host |
| CSCsf99844 | wrong values for current connections using CLI "show resource usage" |
| CSCsg64119 | rule's keyword editor treats NOT as binary rather than unary |
| CSCsg73786 | Devices should not be added to MARS if Discovery is unsuccessful |
| CSCsg76958 | FR: Recognize either CIPS network variables or have CSMARS net variables |
| CSCsg82600 | some syslog results in unknownDET with 'Activate' |

| Reference Number | Description |
|---|---|
| CSCsh00013 | Case Management: history does indicate change of ownership |
| CSCsh44351 | CSM multiple hostname matches failed to return multiple hosts |
| CSCsh73553 | MARS DVD imaging does not support USB keyboard |
| CSCsh97060 | MARs says it can delete up to 500 at a time but only lets you delete 50. |
| CSCsi07186 | User can input unsupported characters in AAA device name |
| CSCsi11312 | pn_incident_log and pn_report_log should be archived |
| CSCsi13100 | gui.sh dev build makes different JBOSS web.xml than make release |
| CSCsi18757 | CS-MARS - Request to have the "ssldump" command in the MARS CLI. |
| CSCsi29398 | CS-Mars does mitigate to the proper endpoint |
| CSCsi49285 | Mismatch in results between query and report. |
| CSCsi49330 | Mismatch in results between query and report when query is based on user |
| CSCsi49396 | Mismatch in results between query & report when query based on desti. IP |
| CSCsi49419 | The application hangs, while getting the results for a query. |
| CSCsi49474 | Mismatch results between query and report (custom column) |
| CSCsi51999 | Edit SW based Application device need submit twice |
| CSCsi52731 | mars reboots w/o asking for confirmation after user clicked cfg update |
| CSCsi62384 | The performace test kills all the process during the weekend run |
| CSCsi65713 | Index needs to be removed for the pn_report_result table |
| CSCsi65960 | L2 mitigation has problem finding path |
| CSCsi68126 | For multiple context mode, inbound/outbound error reports are incorrect. |
| CSCsi69310 | security hole happens if users close browsers without click logout |
| CSCsi86420 | with 60% event rate capacity, query events ranked by time takes 20 min |
| CSCsi91734 | Mismatch in results between query and report for All Matching Events |
| CSCsi93283 | Mismatch between query and report results for source port ranking. |
| CSCsj15512 | Update reports when handling deletion of hosts |
| CSCsj20697 | LC did not get added to GC so unable to generate syslogs. |
| CSCsj23845 | CS-MARS Action filter doesn’t work if not associated with incidents |
| CSCsj28376 | Box may not be able to reboot after recovery, under certain conditions |
| CSCsj51240 | Paging does not work for report right after adding it to a case. |
| CSCsj66955 | scheduled discovery is scheduled at wrong time |
| CSCsj69985 | Syslogrelay is accepting same IP for both source and collector |
| CSCsj90505 | Inline/Batch query not match on NAT connection report |
| CSCsj90875 | Inline/Batch query: result mismatch on Matched Rule Ranking |
| CSCsj96592 | Adding LC with version lower than 4.3.1 should version mismatch err |
| CSCsk04282 | MARS failed to import 1000 hosts vulnerablilty information |
| CSCsk26308 | pink error when listing devices while scalability script running |
| CSCsk27276 | MARS: Isolated Networks in Topology due to ’ip unnumbered’ Interface |

| Reference Number | Description |
|---|---|
| CSCsk39645 | GUI doesn't check duplicate agent ip address when adding application |
| CSCsl58216 | MARS Layer 2 path and mitigation issues with IOS 12.3 and 12.4 version |
| CSCsm40349 | rare crashing issue due to file system check/memory short |
| CSCso39840 | Sud incr. in traf raw msg should have std deviation instead of variance |
| CSCso40549 | L2 path through 7600 with VRF give error message |
| CSCso54308 | LC stops communincating to GC, stack dump shows stuck in Version Check |
| CSCso59056 | pnrestore throws the warning of archive version 0 |
| CSCso97681 | Host name appears inconsistently on Incident Vector Topology |
| CSCsq57230 | custom parser performance issue |
| CSCsq69190 | 4.3.5 eth1 IP address not migrated to 5.3.5 |
| CSCsq75966 | Actual Time For 'pnexp' Or 'pnimp' Is Much Higher Than Estimated |
| CSCsq88032 | Anomaly baselines are not part of archive/restore data |
| CSCsr41052 | MARS not showing the switches in L2 mitigation path consistently |
| CSCsv10459 | Rawmsg retrieve Stop(from the GUI) does not stop backend immediately |
| CSCsv40163 | MARS adding wrong device entry after adding ISS Provetia as ISS RS 7.0 |
| CSCsv40163 | MARS adding wrong device entry after adding ISS Provetia as ISS RS 7.0 |
| CSCsv66667 | MARS not printing the correct Layer 2 topology |
| CSCsw36540 | CSM-MARS linkage is not working when AAA is configured as Authentication |
| CSCsw77193 | MARS: Documentation on setting up NFS archiving with NetApp wrong |
| CSCsw80468 | Querying events filter by severity level not generating any reports |
| CSCsw86766 | Graphgen crashes periodically on memory "new" and "delete" |
| CSCsx01576 | Unable to parse NAC 4.5 |
| CSCsx01964 | CS-MARS Seconds field in Time range for rules not working correctly. |
| CSCsx27968 | Adding large number of devices to the rule handled ungracefully |
| CSCsx43819 | Unknown Device Event Types from FWSM 3.1 |
| CSCsx48107 | Graphgen crashed when it tried to compute path for an incident |
| CSCsx48620 | MARS 6.0.2 Issue with modifying user roles. |
| CSCsx51498 | the deleted devices are still showing in the resource utilization report |
| CSCsx51554 | OpenSSL changes for incorrect checks for malformed signatures |
| CSCsx68259 | MARS device support for Check Point NG FP3 |
| CSCsx76900 | MARS raid firmware hangs |
| CSCsx77718 | Unresponsive SFTP archive server causes some zombie processes |
| CSCsx80409 | csv report times out for custom column batch query |
| CSCsx95786 | User defined rule doesn't work for keyword with NOT condition |
| CSCsy00859 | Custom parser cannot over ride a generic Linux event |
| CSCsy15761 | Unable to see SNMP Health traps from IPS devices |
| CSCsy18297 | DbSysParam setnum value should handle long values |

| Reference Number | Description |
|---|---|
| CSCsy24991 | CS-MARS exported .csv reports save as .htm unless changed to .csv |
| CSCsy32973 | System Error (pink box) for Management or Incidents tab |
| CSCsy37111 | Every ~20 min processes restart when environment slows port scans |
| CSCsy45872 | Unknown Device Event Type for ACS 4.2 |
| CSCsy46243 | Mis-Mapped IPS events in MARS for signature 13492/0 |
| CSCsy56644 | Mars 6.0.1 - java stack trace seen query results |

# Resolved Caveats —Release 6.0.3

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

| Reference Number | Description |
|---|---|
| CSCpn01489 | BQ: Query summary doesn’t mention "severity" if it’s a criterion |
| CSCsc15590 | MARS not including all events in a report, query returns events fine |
| CSCsc95831 | log messages of MARS processes stopped being written into backend log |
| CSCsg52561 | ability to customize the content of a notification event not just links |
| CSCsg53193 | CS-MARS - Recent Incidents for Last field wastes space |
| CSCsh68381 | Bogus message when editing device name |
| CSCsi30795 | CS-Mars - 56 unknown ASA 7.2 Syslog events or parsing errors |
| CSCsj79859 | Unsupported events for PIX/ASA |
| CSCsk40888 | ASA/PIX - Some new msgs not parsed |
| CSCsm38062 | MARS change wrong device type when use SNMP as access type |
| CSCsm71150 | Incidents page doesnt show all incidents when checked from summary tab. |
| CSCso69634 | Query Criteria for Event Types unnecessarily slow in GUI |
| CSCsq34564 | Manual implys that just 1 interface can be used for traffic |
| CSCsq60315 | Netscreen discovery with hostname unset shows incorrect error message |
| CSCsq75890 | GUI accepting network as a next hop address |
| CSCsr46945 | LC Delete takes too long with lots of global networks |
| CSCsr48639 | WLC events are not getting parsed - Inconsistent behaviour |
| CSCsr50272 | Output of Ifconfig ? On CLI |
| CSCsr55407 | Event mapping is not correct for few of the ACS failed auth events |
| CSCsr97564 | Netflow receive fails on some pnparser startups due to port bind failure |
| CSCsu01818 | Intrushield sensor device name field should take sensor DNS name |
| CSCsu38616 | LM_ERROR@./pnesloader\.. TarFile: Write to closed file: should be INFO |
| CSCsu47813 | ASA 8.1.2 Netflow for short lived session are not sessionizing in MARS |
| CSCsu56289 | Cat6k WiSM module support for mars 6.0.2 release |
| CSCsu65367 | pnupgrade from GUI sometimes receives SIGPIPE signal |
| CSCsu83902 | Custom Parser is not working for McAFee EPO SNMP TRAP |

| Reference Number | Description |
|---|---|
| CSCsu98563 | Wireless LAN controller SNMP messages fill up backend log. |
| CSCsv05921 | customer can not import the exported file for 4.3.6 to 6.0.1 migration |
| CSCsv40163 | MARS adding wrong device entry after adding ISS Provetia as ISS RS 7.0 |
| CSCsv43369 | Inline queries, batch queries and reports can be sped up |
| CSCsv50303 | Wrong mail server config caused MARS to stop firing incidents |
| CSCsv56003 | MARS 6.x supports weak encryption |
| CSCsv65003 | Can not download IPS packet capture log with real time raw events. |
| CSCsv68502 | %ASA-3-403502 syslog in ASA 7.0 is not getting parsed |
| CSCsv69537 | clicking "show" in the false positive page throws system error |
| CSCsv72863 | IPS Signature Dynamic update is not working. |
| CSCsv74330 | inaccurate time range while retrieving the raw message files |
| CSCsv74993 | malformed snmp trap causes pnparser to crash or parse/store junk values |
| CSCsv75723 | CCO test connectivity failure should not fire sig download failure event |
| CSCsv78151 | MARS-3-100069 event for IPS sig update not correctly parsed by MARS. |
| CSCsv78602 | MARS shouldn’t download IPS pkg version smaller than current IPS version |
| CSCsv82965 | Observed following problem while uploading ASA device with Seed file |
| CSCsv83497 | RAID BBU Replacement Notification |
| CSCsv85877 | Pink box error while adding and discovering the device with the same IP |
| CSCsv86398 | IPS virtual sensors are not handled in the inactive reporting algorithm |
| CSCsv89508 | MARS Password Attack/Scan Incidents fire containing ARP Collision Events |
| CSCsv93835 | Some of the ASA 8.0 messages (old) are not Parsing |
| CSCsv94686 | User report Edit should open report name edit window. |
| CSCsv94963 | Documentation update required for scheduled/on-demand reports. |
| CSCsv96026 | The word "Exchange" should not be there in pnupgrade help. |
| CSCsv96741 | Query results not correct when TR-RR filters are used. |
| CSCsw14613 | Graphgen is running at high cpu usage 95%+ |
| CSCsw17192 | Parsing errors in few ASA7.2 syslog messages |
| CSCsw20399 | Update MARS copyrite to 2009 in the GUI |
| CSCsw21274 | CVE details not correctly updated for event ID 1905170. |
| CSCsw22879 | Upgrade openssh to version 3.9p1-11.el4_7. |
| CSCsw24104 | Device Event ID and severity not correct for event 5502464 in MARS. |
| CSCsw24148 | ASA 804, Some of the message are not parsed properly |
| CSCsw25387 | Improve performance for Incidents page and Summary page |
| CSCsw41174 | A tool to verify and check the health of exported/archived config file |
| CSCsw41549 | Expand situations for choice of either inline or batch query |
| CSCsw53316 | Adding ASA 7.0 or ASA 7.2 throwing Pink box error. |
| CSCsw63871 | MARS should monitor and restart event processing when it stops |

| Reference Number | Description |
|---|---|
| CSCsw64685 | MARSCatalog.xml file should include data version as well as binary |
| CSCsw65261 | ASA/PIX - ESMTP syslog messages showing protocol as N/A instead of TCP |
| CSCsw67019 | Need to include a script during upgrade |
| CSCsw88400 | 6.0 User Guide needs to updated with Raw Message Retrieval Section |
| CSCsx08060 | NAC 4.1 parser - wrong event description for Event ID 2200007 |
| CSCsx08277 | mars20, eth0 and eth1 got swapped after reboot |
| CSCsx16387 | Enable License Check for New Flash Drive - MARS 25/55 |
| CSCsx19439 | superV puts a runaway program to the stopped list |
| CSCsx20877 | MARS: URLF-6-URL_ALLOWED event-type parsing failure |
| CSCsx23614 | Roadmap Doc has bad link to wrong doc |
| CSCsx25085 | start time in the future error when restore Jan data |
| CSCsx27739 | pink box showed up after incident tab is clicked |
| CSCsx30276 | need mars hostname in raid BBU email notification |
| CSCsx30366 | typo in BBU failure notification email |
| CSCsx31425 | IPS sig update fails if pkg name is not specified on the local server |
| CSCsx40408 | LC and GC communication ports should contain protocols |
| CSCsx53137 | pink box while editing Device Event Type. |
| CSCsx55011 | MARS is not emailing the session data in incident XML Notification |
| CSCsx58525 | Process process_inlinerep_srv crashes continously on high EPS. |
| CSCsx67582 | superV needs to handle zombie backend processes |
| CSCsx68559 | High CPU Utilization in pnparser sessionization in corner case scenario |
| CSCsx70978 | Scheduled report of incidents rank by time have no result returned |
| CSCsx74273 | upgrade.log file is missing in error logs file |
| CSCsx80489 | Seedfile documentation needs to be updated. |
| CSCsx83331 | Mars pnparser stopps working |
| CSCsy13632 | Doc: Need to reboot Archiving server after configuration |
| CSCsy32085 | DOC: Installation Guide needs clarification on SFTP remote path field |
| CSCsy49888 | All matching events with eventtype criteria doesn't give accurate result |

## Resolved Caveats —Releases Prior to 6.0.3

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