



# Release Notes for Cisco Security MARS Appliance 6.0.7

---

**Last Published: July 19, 2010**



**Note**

---

We sometimes update the printed and electronic documentation after original publication. Therefore, you should review the documentation on [Cisco.com](http://Cisco.com) for any updates.

---

These release notes are for use with the Cisco Security Monitoring, Analysis, and Response System (MARS), Release 6.0.7, running on any supported MARS Appliance model listed in [Supported Hardware, page 2](#).

This chapter contains the following topics:

- [Introduction, page 1](#)
- [Supported Hardware, page 2](#)
- [New Features, page 2](#)
- [Upgrade Instructions, page 4](#)
- [Documentation Errata, page 7](#)
- [Important Notes, page 7](#)
- [Caveats, page 9](#)
- [Product Documentation, page 12](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 12](#)

## Introduction

Release 6.0.7 is now available as an upgrade of 6.0.6 of your software release in support of the MARS Appliance models as identified in [Supported Hardware, page 2](#). Registered SMARTnet users can obtain release 6.0.7 from the Cisco support website at the following URL:

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

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



---

**Americas Headquarters:**

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

# Supported Hardware

Release 6.0.7 supports the following Cisco Security MARS Appliance models:

## Local Controller Appliances: 2<sup>nd</sup> 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 110RF (CS-MARS-110RF-K9)
- Cisco Security MARS 110 (CS-MARS-110-K9)
- Cisco Security MARS 210 (CS-MARS-210-K9)

## Local Controller Appliances: 1<sup>st</sup> 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: 2<sup>nd</sup> Generation

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

## Global Controller Appliances: 1<sup>st</sup> Generation

- Cisco Security MARS GCm (CS-MARS-GCM-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 changes and enhancements:

- [Changes and Enhancements, page 2](#)
- [New Vendor Signatures, page 3](#)

# Changes and Enhancements

The following enhancement exists in Cisco Security MARS, Release 6.0.7:

- **Support for Windows 2008**—Cisco Security MARS provides agent based, native log support for Windows 2008 server hosts. Users can send syslog to CS-MARS by installing a Snare agent on their Windows 2008 server hosts.
- **Support for Windows IIS 7**—Cisco Security MARS provides support for IIS 7 on Windows 2008 servers.

**Note**

If you are upgrading from Windows 2003 to Windows 2008, ensure that any ancillary devices and software you employ are supported. For more information see [Supported and Interoperable Devices and Software for Cisco Security MARS Local Controller 6.0.x](#).

## New Vendor Signatures

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

Revised in 6.0.7	Product	Signature Version Supported
<b>Intrusion Prevention and Detection Signatures</b>		
Yes	Cisco IDS 4.0 Cisco IPS 5.x Cisco IPS 6.x Cisco IPS 7.x	Current through S467 signature release. Current as of March 9, 2010.
Yes	Cisco ASA	Current as of March 9, 2010.
Yes	Cisco IOS 12.2/12.4	Current as of March 9, 2010.
Yes	Snort NIDS 2.8	Current through the March 4, 2010 signature release. Latest signature mapped: 16432.
Yes	ISS RealSecure Network Sensor 6.5 and 7.0, and ISS RealSecure Server Sensor 6.5 and 7.0	XPU 30.030 Release date: March 9, 2010
Yes	McAfee IntruShield 4.1	v4.1.69.4 Release date: March 9, 2010
Yes	McAfee Enterecept HIDS 6.x	Current through the March 9, 2010 signature release.
Yes	CheckPoint Application Intelligence (VPN-1 NG with Application Intelligence R65)	Current through the March 9, 2010 signature release.
Yes	Netscreen IDP 2.1, 3.0, 3.1, 4.0, 4.1	Signature version: 4.0 Release date: December 10, 2009
No. EOS.	Symantec NIDS, v 4.0	Signature package: 95 Release date: June 12, 2008
Yes	Enterasys Dragon 6.x, 7.x	Current through the March 3, 2010 signature release.
No. EOS.	Symantec Manhunt 3.x (See Symantec NIDS, v 4.0.) 3.4.3 Update 59	3.4.3 Update 59 Current through the May 24, 2007 signature release.
<b>Vulnerability Scanner Signatures</b>		
Yes	Qualys Guard ANY	Current through the March 9, 2010 signature release.
Yes	E-Eye, Retina Scanner Vulnerability Software, version 5.6	Current through the March 9, 2010 signature release.
Yes	Foundstone, version ANY	Current through the March 2, 2010 signature release.

Revised in 6.0.7	Product	Signature Version Supported
Yes	Common Vulnerabilities and Exposures (CVE) Database	Current with the March 9, 2010 definition update.
<b>Miscellaneous Support</b>		
No	Oracle 11g	Support for new AUDIT_ACTIONS.

<sup>1</sup> 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 to 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 following general notes apply to this release:

- If you are upgrading from Windows 2003 to Windows 2008, ensure that any ancillary devices and software you employ are supported. For more information see [Supported and Interoperable Devices and Software for Cisco Security MARS Local Controller 6.0.x](#).
- When downloading software packages from CCO to MARS, ensure that your credentials (username or password) do not include the ampersand (&) character. The credential will be truncated before being passed to the authentication module, which results in an error message about invalid user credentials.
- The CS-MARS 110R running the FIPS-compliant card *cannot* be managed by a Global Controller.
- The MARS Appliance performs a file system consistency check (fsck) on all disks when either of the following conditions is met:
  - The system has not been rebooted during the past 180 days.
  - 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 6.0.7

If you are upgrading from Windows 2003 to Windows 2008, ensure that any ancillary devices and software you employ are supported. For more information see [Supported and Interoperable Devices and Software for Cisco Security MARS Local Controller 6.0.x](#).

## Upgrade to 6.0.6

No important notes exist for the 6.0.6 upgrade.

## Upgrade to 6.0.5

The 6.0.5 release is a general bug fix and signature update release for all MARS appliance models. However, it offers new functionality for an existing CS-MARS 110R when you order and install a FIPS-compliant PCI card. Once installed, you can configure FIPS-specific features within MARS. For more information, see the [CS-MARS FIPS PCI CARD Quick Install](#) document.

## Upgrade to 6.0.4

No important notes exist for the 6.0.4 upgrade.

## 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, 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 are ignored. The "restricted" models 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	<i>Migration required.</i> See <a href="#">Migrating Data from Cisco Security MARS 4.x to 6.0.1</a>
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-6.0.3.3186.zip
6.0.3	6.0.4	csmars-6.0.4.3229.zip
6.0.4	6.0.5 no FIPS support	csmars-6.0.5.3358.iso/zip
	6.0.5 with FIPS support	csmars-6.0.5.3361-FIPS.iso/zip
6.0.5	6.0.6	csmars-6.0.6.3367.zip
6.0.6	6.0.7	csmars-6.0.7.3403.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 the Download Software page, 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/web/siteassets/account/index.html>

## Documentation Errata

N/A.

## 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
<a href="#">CSCsc50636</a> , <a href="#">CSCsc50652</a>	<p><i>Issues:</i> 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:</p> <ul style="list-style-type: none"> <li>• In release 4.2.1 and earlier, the process names are pnids50_srv and pnids40_srv.</li> <li>• In release 4.2.2 and later, the process is named csips.</li> </ul> <p>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.</p> <p><i>Workaround:</i> 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:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>
<a href="#">CSCpn02175</a>	<p><i>Issue:</i> 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.</p>
<a href="#">CSCpn02073</a>	<p><i>Issue:</i> After renaming a cloud, clicking the cloud again causes an error.</p> <p><i>Workaround:</i> Refresh the page before clicking a renamed cloud.</p>
<a href="#">CSCpn01270</a>	<p><i>Issue:</i> The free-form search may not work for the following devices:</p> <ul style="list-style-type: none"> <li>• Check Point Opsec NG FP3</li> <li>• Cisco CSA, 4.0</li> <li>• Cisco, IDS, 3.1 and 4.0</li> <li>• ISS, RealSecure, 6.5 and 7.0</li> <li>• Entercept Entercept, 2.5 and 4.0</li> <li>• IntruVert IntruShield, 1.5</li> </ul>
<a href="#">CSCpn00247</a>	<p><i>Issue:</i> The automatic time-out feature built into the GUI does not work when the Summary page is left open with automatic refresh selected.</p> <p><i>Resolution:</i> Please log out of the system when you are no longer using it.</p>

# 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, page 9](#)
- [Open Caveats— Release 6.0.7, page 10](#)
- [Resolved Caveats —Release 6.0.7, page 12](#)
- [Resolved Caveats —Releases Prior to 6.0.7, page 12](#)

## Open Caveats for Supporting Devices

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

Reference Number	Description
<b>Cisco Security Manager</b>	
<a href="#">CSCsm96376</a>	Policy lookup icon not shown if device is deleted from MARS
<a href="#">CSCsm94537</a>	Policy lookup icon not shown for a device deleted and re-added to MARS
<a href="#">CSCsm43237</a>	Minimum password length for Security Manager account in MARS
<a href="#">CSCsf31401</a>	MARS query does not highlight rules inside any policy group named Local
<b>Firewall Services Module</b>	
<a href="#">CSCsl27574</a>	FWSM Syslog message FWSM-6-302013 with wrong Real and Mapped IP

## Open Caveats— Release 6.0.7

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

Reference Number	Description
CSCpn01398	Unable to shutdown an interface
CSCsb77550	CSV-re import of CSA and Symantec agents unsuccessful
CSCsc90480	MARS Incident notification options are not configurable
CSCsd61749	pnrestore doesn't restore all of the system config
CSCsd84350	CS-MARS/CSM: Credentials change on CSM side not checked.
CSCsd89457	Incorrect handling of time range for rules that fire periodically.
CSCse10945	Summary Page Graphs Spontaneously Change Displayed Size (w/ multi-head)
CSCse31722	Cloud toggle only works on first page of reporting devices
CSCse42953	CS-Mars - unable to show L2 path when source and destination in same net
CSCse98029	Occasionally corrupted event data enters into MARS database
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
CSCsh44351	CSM multiple hostname matches failed to return multiple hosts
CSCsh97060	MARS says it can delete up to 500 at a time but only lets you delete 50.
CSCsi18757	CS-MARS - Request to have the "ssldump" command in the MARS CLI.
CSCsi29398	CS-Mars does mitigate to the proper endpoint
CSCsi68126	For multiple context mode, inbound/outbound error reports are incorrect.
CSCsj15066	Report is not emailed because Message exceeds maximum fixed size
CSCsj23845	CS-MARS Action filter doesn't work if not associated with incidents
CSCsk04282	MARS failed to import 1000 hosts vulnerability information
CSCsk27276	MARS: Isolated Networks in Topology due to 'ip unnumbered' Interface
CSCsl58216	MARS Layer 2 path and mitigation issues with IOS 12.3 and 12.4 version
CSCso01260	Loading hosts from seed file does not fill interface information on MARS
CSCso30992	Entire GUI stops working after adding a device with same name as MARS
CSCso97681	Host name appears inconsistently on Incident Vector Topology
CSCsq57230	Custom parser performance issue
CSCsq75966	Actual Time For 'pnexp' Or 'pnimp' is much higher than estimated
CSCsr41052	MARS not showing the switches in L2 mitigation path consistently
CSCsu42351	MARS: Hotswap remove allows both disks in a redundant pair to be removed
CSCsv10459	Rawmsg retrieve Stop (from the GUI) does not stop backend immediately
CSCsv23244	Unable to edit Cisco Switch IOS event parser in 6.0.1 DSF feature.
CSCsv40163	MARS adding wrong device entry after adding ISS Provetia as ISS RS 7.0

Reference Number	Description
<a href="#">CSCsv66667</a>	MARS not printing the correct Layer 2 topology
<a href="#">CSCsw36540</a>	CSM-MARS linkage is not working when AAA is configured as Authentication
<a href="#">CSCsw80468</a>	Querying events filter by severity level not generating any reports
<a href="#">CSCsx01576</a>	Unable to parse NAC 4.5
<a href="#">CSCsx48620</a>	MARS 6.0.2 Issue with modifying user roles.
<a href="#">CSCsx51498</a>	The deleted devices are still showing in the resource utilization report
<a href="#">CSCsx68259</a>	MARS device support for Check Point NG FP3
<a href="#">CSCsx95786</a>	User defined rule doesn't work for keyword with NOT condition
<a href="#">CSCsy15761</a>	Cisco SNMP Traps with enterprise id 9 are parsed incorrectly
<a href="#">CSCsy45872</a>	Unknown Device Event Type for ACS 4.2
<a href="#">CSCsz29163</a>	CS-MARS Single Zone Report Showing Info from other Zones
<a href="#">CSCsz49880</a>	Inactive rules becomes active after importing using DSF
<a href="#">CSCsz56227</a>	Severity not evaluated/matched correctly for CSA and some IPS events
<a href="#">CSCsz78202</a>	Querying IPS events with prot:IP(SNMP traps) generates improper results
<a href="#">CSCsz84861</a>	MARS - 12 path does not show stacked switches
<a href="#">CSCsz85334</a>	Unable to update custom signature package with erroneous XML
<a href="#">CSCsz85727</a>	Wrong info on popup while deleting a site on GC.
<a href="#">CSCta07951</a>	Older unsupported versions of Checkpoint should not be supported in MARS
<a href="#">CSCta09391</a>	CS-MARS-6.0-Filtering on Red severity slow and Oracle process 100%
<a href="#">CSCta49936</a>	GC report with BTF site reference is always stays in progress.
<a href="#">CSCta74645</a>	ASA site report takes a few seconds to display even on a non-busy box
<a href="#">CSCta96180</a>	Invalid credential error if CCO passwd including URL special characters
<a href="#">CSCtb12268</a>	DSF export/import feature for rules/report with sites is not working
<a href="#">CSCtb39169</a>	MARS 6.0.x pulling of IDS 4.x sensors not working via rdep
<a href="#">CSCtb69227</a>	CSM device causing query pink box
<a href="#">CSCtb92648</a>	Custom column query with keyword doesn't return results
<a href="#">CSCtc25411</a>	MARS: Oracle polling interval is ignored when connections are limited
<a href="#">CSCtc41087</a>	MARS does not validate the date on the IPS certificate
<a href="#">CSCtd10574</a>	Severity not evaluated/matched correctly for CSA events.
<a href="#">CSCtd15002</a>	CS-MARS: IOS IPS Sig 5733 Maps to "WWW IIS Internet Printing Overflow"
<a href="#">CSCte98430</a>	Custom signatures not applied toward sensors configured as IPS 7.x
<a href="#">CSCtf18192</a>	MARS cannot retrieve AP hostname correctly via SNMP
<a href="#">CSCtf51945</a>	Oracle procedures pn_pack_rr_ie1/pn_pack_rr_ie2 are missing
<a href="#">CSCtf52128</a>	Pink Box error when clicking on Configuration Information
<a href="#">CSCtg07158</a>	Large # of sessions per incident may cause graphgen to hang Mars
<a href="#">CSCtg23469</a>	MARS upgrades, IPS signature updates, and reports may fail with error
<a href="#">CSCtg30989</a>	MARS: pntstore times out with large number of days archived in NFS

## Resolved Caveats —Release 6.0.7

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

Reference Number	Description
<a href="#">CSCsm40349</a>	Rare crashing issue due to file system check/memory short
<a href="#">CSCsr68236</a>	Device events sometime fail to map to MARS event types
<a href="#">CSCtc05633</a>	Cross launching from CSM causes LC / GC certificate issues
<a href="#">CSCte44085</a>	MARS: Will not start with large NAT/ACL tables
<a href="#">CSCte46251</a>	MARS: Windows Pull fails, Domain name is surrounded by single-quotes (')
<a href="#">CSCte66589</a>	Data archiving requests not held during partition unmount
<a href="#">CSCtf04414</a>	Pnarchiver leaking memory and causing high CPU utilization
<a href="#">CSCtf25480</a>	MARS: 6.x CLI hotswap takes ? as disk 0
<a href="#">CSCtf52041</a>	Pnparser service will not stay running
<a href="#">CSCtf73095</a>	Very large PN_audit_log table causes Java to run @ 99% CPU
<a href="#">CSCth85541</a>	Upgrade with SFTP archiving configured may hang in rare cases

## Resolved Caveats —Releases Prior to 6.0.7

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

- [http://www.cisco.com/en/US/products/ps6241/prod\\_release\\_notes\\_list.html](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](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>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

