Release Notes for Cisco Security MARS Appliance 6.1.7

Last Published: December 10, 2012

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 6.1.7, running on any supported MARS Appliance model listed in Supported Hardware, page 2.

This chapter contains the following topics:

Introduction

Release 6.1.7 is now available as an upgrade of 6.1.6 of your software release in support of the MARS Appliance models as identified in Supported Hardware, page 2. Registered SMARTnet users can obtain release 6.1.7 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 6.1.7 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 GCm (CS-MARS-GCM-K9) as a MARS GC
- Cisco Security MARS GC (CS-MARS-GC-K9)

New Features

This release contains no new features. It is a release dedicated to signature updates.

Changes and Enhancements

All changes made in this release are related to the signatures.

New Vendor Signatures

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

Revised in 6.1.7	Product	Signature Version Supported
Intrusion Prevention and Detection Signatures		
Yes	Cisco IDS 4.0 Cisco IPS 5.x Cisco IPS 6.x Cisco IPS 7.x	Current through S675 signature release. Current as of Oct 23, 2012.
No	Cisco ASA	Current as of April, 2011.
No	Cisco IOS 12.2/12.3/12.4	Current as of November 3, 2011.
Yes	Snort 2.9	Current as of September 18, 2012 Latest signature mapped: 24155
Yes	ISS RealSecure Network Sensor 6.5 and 7.0, and ISS RealSecure Server Sensor 6.5 and 7.0	XPU 32.100 Release date: October 10, 2012
No	McAfee Intruvert	v4.1.83.12 Release date: March 23, 2011
No	McAfee Entercept HIDS 6.x	Current through the July 26, 2011 signature release.
No	CheckPoint Application Intelligence (VPN-1 NG with Application Intelligence R65)	Current through the August 23, 2011 signature release.
Yes	Juniper IPS	Signature version: 5.1 Release date: July 18, 2012
Yes	Netscreen IDP 3.x	Signature version: 5.1 Release date: October 17, 2012
Yes	Enterasys Dragon 7.2/7.3	Current through the October 17, 2012 signature release.
Vulnerability Scanner Signatures		
Yes	Qualys Guard ANY v6.7.20-1	Current through the October 23, 2012 signature release.
Yes	E-Eye, Retina Scanner Vulnerability Software, version v5.14.1.2434	Current through the October 23, 2012 signature release.
No	Foundstone, version ANY	Current through the March 2, 2011signature release.
Yes	Common Vulnerabilities and Exposures (CVE) Database	Current with the October 25, 2012 definition update.
Miscellaneous Support		
No	Oracle 11g	Support for new AUDIT_ACTIONS.

Upgrade Instructions

The MARS upgrade packages are the primary vehicle for major, minor, and patch software releases. 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 installation, 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 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.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 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 6.1.6

No important notes exist for the 6.1.6 upgrade.

Upgrade to 6.1.5

No important notes exist for the 6.1.5 upgrade.

Upgrade to 6.1.4

No important notes exist for the 6.1.4 upgrade.

Upgrade to 6.1.3

No important notes exist for the 6.1.3 upgrade.

Upgrade to 6.1.2

No important notes exist for the 6.1.2 upgrade.

Upgrade to 6.1.1

No important notes exist for the 6.1.1 upgrade.

Upgrade to 6.0.8

No important notes exist for the 6.0.8 upgrade.

Upgrade to 6.0.7

No important notes exist for the 6.0.7 upgrade.

Upgrade to 6.0.6

No important notes exist for the 6.0.6 upgrade.

Upgrade to 6.0.5

No important notes exist for the 6.0.5 upgrade.

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 .

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 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-6.0.3.3186.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
6.0.7	6.0.8	csmars-6.0.8.3427.zip
6.0.8	6.1.1	csmars-6.1.1.3445.zip
6.1.1	6.1.2 no FIPS support	csmars-6.1.2.3466.zip
	6.1.2 with FIPS support	csmars-6.1.2.3466.iso
6.1.2	6.1.3	csmars-6.1.3.3501.zip
6.1.3	6.1.4	csmars-6.1.4.3506.zip
6.1.4	6.1.5	csmars-6.1.5.3508.zip
6.1.5	6.1.6	csmars-6.1.6.3511.zip
6.1.6	6.1.7	csmars-6.1.73515.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

The *Cisco Security MARS 6.x Documentation Guide and Warranty* details user documentation for this release.

Important Notes

No important notes exist for the 6.1.7 upgrade.

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
Firewall Services Module	
CSCsl27574	FWSM Syslog message FWSM-6-302013 with wrong Real and Mapped IP

Open Caveats— Release 6.1.7

None

Resolved Caveats —Release 6.1.6

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

Reference Number	Description

Open Caveats— Release 6.1.6

None

Resolved Caveats —Release 6.1.6

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

Reference Number	Description
CSCua96907	CS-MARS 6.1.5 ASA Botnet rule association missing & botnet graphs empty
CSCtz71398	IPS Dynamic Sig Update Failed

Open Caveats— Release 6.1.5

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

Reference Number	Description
CSCtw56499_	MARS - GC/LC communication disruption can result in out-of-sync objects
CSCtx01503	Unknown device event type when combining custom parser with builtin
CSCty03556	MARS GUI login failure syslog message shows 0.0.0.0 as user IP address
CSCty23264	*eventSharedBuffer* reader for *process_event_srv* can get stuck
CSCtw56499	MARS - GC/LC communication disruption can result in out-of-sync objects
CSCtz17737	Reports shown by CS-MARS list incorrect (old) hostnames for IP addresses

Resolved Caveats —Release 6.1.5

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

Reference Number	Description
CSCtu14120	The /tmp directory can get filled with config files

Resolved Caveats —Releases Prior to 6.1.4

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 road map:

- *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

Note The Documentation Guide and Cisco.com link to the most recent Cisco Secure MARS publications. The release number for many documents may vary from the current release number.

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.