Release Notes for Cisco Security MARS Appliance 6.1.1

Last Published: Nov 16, 2010

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

This chapter contains the following topics:

Introduction

Release 6.1.1 is now available as an upgrade of 6.0.8 of your software release in support of the MARS Appliance models as identified in Supported Hardware, page 2. Registered SMARTnet users can obtain release 6.1.1 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 6.1.1 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

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

ASA 8.2.2 Botnet Traffic Filter

The ASA BTF feature was enhanced in ASA 8.2.2 to add blacklist actions including blocking functionality to Dynamic Filter, as well as additional attributes. MARS Release 6.1.1 supports these enhanced BTF attributes:

- Parses the new BTF-specific syslogs that provide visibility into blocked site traffic
- Supports additional attributes for "threat_level" and "threat_category"
- Adds two system rules and one report

ASA 8.2.3

In 6.1.1, CS-MARS supports ASA 8.2.3 (Spyker) CLI changes and high priority syslogs for CS-MARS functionality

Agent-less Windows 2008/Vista/7 Support

In Windows 2008/Vista/7, the Windows Event Log subsystem was substantially overhauled relative to earlier versions supported by CS-MARS. MARS 6.1.1 supports Windows 2008/Vista/7 events pulled by CS-MARS from the Windows hosts (agent-less). [In 6.0.7, MARS supported Windows 2008/Vista/7 events sent by a SNARE agent (agent-based).]

Ability to Manage SSH Keys

A new CLI command is implemented to handle outdated SSH keys: **pnsshfs**

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.x.

New Vendor Signatures

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

Revised in 6.1.1	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 S496 signature release. Current as of September 1, 2010.
Yes	Cisco ASA	Current as September, 2010.
No	Cisco IOS 12.2/12.3/12.4	Current as of March 9, 2010.
Yes	Snort 2.8	Current as of September 7, 2010 Latest signature mapped: 17209.
Yes	ISS RealSecure Network Sensor 6.5 and 7.0, and ISS RealSecure Server Sensor 6.5 and 7.0	XPU 30.080 Release date: August 10, 2010
Yes	McAfee IntruShield 4.1	v4.1.80.22 Release date: August 26, 2010
Yes	McAfee Entercept HIDS 6.x	Current through the August 17, 2010 signature release.
Yes	CheckPoint Application Intelligence (VPN-1 NG with Application Intelligence R65)	Current through the August 30, 2010 signature release.
Yes	Juniper IPD	Signature version: 4.0 Release date:September 9, 2010
No	Netscreen IDP 3.x	Signature version: 4.0 Release date: June 14, 2010

Revised in 6.1.1	Product	Signature Version Supported
Yes	Enterasys Dragon 7.2/7.3	Current through the September 2, 2010 signature release.
Vulnerability Scanner Signatures		
Yes	Qualys Guard ANY	Current through the September 8, 2010 signature release.
Yes	E-Eye, Retina Scanner Vulnerability Software, version v5.11.1.2181	Current through the September 1, 2010 signature release.
No	Foundstone, version ANY	Current through the June 17, 2010 signature release.
Yes	Common Vulnerabilities and Exposures (CVE) Database	Current with the September 10, 2010 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. 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 6.1.1

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.

Upgrade to 6.0.8

No important notes exist for the 6.0.8 upgrade.

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.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 6 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	*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

Table 1 Upgrade Path Matrix (Continued)

From Release	Upgrade To	Upgrade Package
6.0.7	6.0.8	csmars-6.0.8.3427.zip
6.0.8	6.1.1	csmars-6.1.1.3445.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

The following notes apply to the MARS 6.1.1 releases:

- In Windows 2008/Vista/7, the Windows Event Log subsystem was substantially overhauled relative to earlier versions supported by CS-MARS. MARS 6.1.1 supports Windows 2008/Vista/7 events pulled by CS-MARS from the Windows hosts (agent-less). [In 6.0.7, MARS supported Windows 2008/Vista/7 events sent by a SNARE agent (agent-based).]

- In 6.1.1, CS-MARS supports ASA 8.2.2 Botnet Traffic Filter and ASA 8.2.3 (Spyker) CLI changes and high priority syslogs for CS-MARS functionality.

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 6.1.1

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

Reference Number	Description
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 of 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 vulnerablilty 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
CSCsv66667	MARS not printing the correct Layer 2 topology

Reference Number	Description
CSCsw36540	CSM-MARS linkage is not working when AAA is configured as Authentication
CSCsw80468	Querying events filter by severity level not generating any reports
CSCsx01576	Unable to parse NAC 4.5
CSCsx48620	MARS 6.0.2 Issue with modifying user roles.
CSCsx51498	the deleted devices are still showing in the resource utilization report
CSCsx95786	User defined rule doesn't work for keyword with NOT condition
CSCsy45872	Unknown Device Event Type for ACS 4.2
CSCsz29163	CS-MARS Single Zone Report Showing Info from other Zones
CSCsz49880	Inactive rules becomes active after importing using DSF
CSCsz56227	Severity not evaluated/matched correctly for CSA and some IPS events
CSCsz78202	querying IPS events with prot:IP(SNMP traps) generates improper results
CSCsz84861	MARS - l2 path does not show stacked switches
CSCsz85334	Unable to update custom signature package with erroneous XML
CSCsz85727	wrong info on pop up while deleting a site on GC.
CSCta09391	CS-MARS-6.0-Filtering on Red severity slow and Oracle process 100%
CSCta49936	GC report with BTF site reference is always stays in progress.
CSCta74645	ASA site report takes a few seconds to display even on a non-busy box
CSCta96180	Invalid credential error if CCO passwd including URL special characters
CSCtb12268	DSF export/import feature for rules/report with sites is not working
CSCtb39169	MARS 6.0.x pulling of IDS 4.x sensors not working via rdep
CSCtb69227	CSM device causing query pink box
CSCtb92648	Custom column query with keyword doesn't return results
CSCtc25411	MARS: Oracle polling interval is ignored when connections are limited
CSCtc41072	Error messages can show up in upgrade log for duplicate Oracle entries
CSCtc41087	MARS does not validate the date on the IPS certificate
CSCtd02654	IMPORTANT TLS/SSL SECURITY UPDATE
CSCtd10574	Severity not evaluated/matched correctly for CSA events.
CSCtd15002	CS-MARS: IOS IPS Sig 5733 Maps to "WWW IIS Internet Printing Overflow"
CSCte98430	Custom signatures not applied toward sensors configured as IPS 7.x
CSCtf18192	MARS cannot retreive AP hostname correctly via SNMP
CSCtg80984	MARS Sends empty / blank / unknown SNMP community string
CSCth36589	MARS parses SNMP traps incorrectly: Dynamically creates invalid Agents
CSCth96188	MARS custom parser for ACS 5.1 messages over-writes certain fields
CSCti21501	CS-MARS 110R FIPS Card causes Delay in WebGUI
CSCti69274	Security Issue in OpenSSL
CSCtj26601	pnparser crashes on parsing access-list

Resolved Caveats —Release 6.1.1

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

Reference Number	Description
CSCti88336	CS-MARS: Need to keep rule id mapping in-sync after upgrade
CSCti69872	CS-MARS recovery disks all use same SSH RSA2 keys.
CSCti68887	MARS reporting wrong severity for SQL Injection Attacks (Sig 5930)
CSCti48196	Particular event type filtering may cause incorrect query/report result
CSCti17475	SuperV restarting due to unusual # of nsems
CSCti11340	One report type may run very slow
CSCth93845	MARS NFS archiving fails periodically
CSCtg30989	MARS: pnrestore times out with large number of days archived in NFS
CSCsw49187	A user cannot manage the SSH keys for archiving

Resolved Caveats —Releases Prior to 6.1.1

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

- http://www.cisco.com/en/US/products/ps6241/prod_release_notes_list.html

Product Documentation

For the complete list of documents supporting this release, see the release-specific document 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

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.