

Cisco Security Advisory: Multiple Vulnerabilities in Cisco Security Monitoring, Analysis and Response System (CS-MARS)

Advisory ID: cisco-sa-20060719-mars

<http://www.cisco.com/warp/public/707/cisco-sa-20060719-mars.shtml>

Revision 1.0

For Public Release 2006 July 19 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

[Summary](#)
[Affected Products](#)
[Details](#)
[Impact](#)
[Software Version and Fixes](#)
[Workarounds](#)
[Obtaining Fixed Software](#)
[Exploitation and Public Announcements](#)
[Status of this Notice: FINAL](#)
[Distribution](#)
[Revision History](#)
[Cisco Security Procedures](#)

Summary

Cisco Security Monitoring, Analysis and Response System (CS-MARS) software contains vulnerabilities related to third-party software and the command line interface (CLI).

- CS-MARS ships with an Oracle database. The database contains several default Oracle accounts which have well-known passwords. If access to the database is obtained, the default accounts may be used to access sensitive information contained in the database.
- CS-MARS ships with the JBoss web application server. A component of the JBoss installation may allow a remote, unauthenticated user to execute arbitrary shell commands with the privileges of the CS-MARS administrator.

- The CS-MARS CLI contains several vulnerabilities which may allow authenticated administrators to execute arbitrary shell commands with root privileges.

All vulnerabilities addressed in this advisory have been corrected in CS-MARS software version 4.2.1.

Cisco has made free software available to address these vulnerabilities for affected customers. There are no workarounds.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20060719-mars.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

This section provides details on affected products.

☐ Vulnerable Products

CS-MARS software versions prior to 4.2.1 are affected by vulnerabilities addressed in this advisory.

To verify the version of CS-MARS software, use an SSH client to login into the system administration command line interface with the **pnadmin** account and execute the **version** command.

```
prompt$ ssh pnadmin@10.0.0.1
pnadmin@10.0.0.1's password:
Last login: Tue Jun 20 16:22:34 2006 from 10.0.0.2

CS MARS - Mitigation and Response System

? for list of commands

[pnadmin]$ version
4.1.5 (2198)
```

☐ Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected these vulnerabilities.

[Top of the section](#) [Close Section](#)

☐ Details

Cisco Security Monitoring, Analysis and Response System (CS-MARS) is a security system that receives event logs from various network devices, correlates and analyzes the received data for security problems, and reports the findings. In addition, CS-MARS can perform automated tasks to mitigate security problems.

- CS-MARS utilizes an Oracle database to store sensitive network event and configuration data. The information contained in the database potentially includes authentication credentials for network devices such as firewalls, routers and IPS devices and the details of network security events. By default, Oracle databases contain several built-in accounts

with well-known passwords. If access can be gained to the database, the accounts could potentially be used to compromise the information stored in the database. The CS-MARS appliance is hardened to prevent local and remote unauthorized access to the database. As a precaution, the database accounts have been disabled by Cisco to prevent abuse should a method to access the database be discovered. The CS-MARS application does not use the default Oracle database accounts. This vulnerability is documented by Cisco bug ID [CSCsd16256](#) ([registered](#) customers only) .

- CS-MARS contains an installation of the JBoss web application server. It may be possible for a remote, unauthenticated user to create a specially-crafted HTTP request which executes arbitrary shell commands on the CS-MARS appliance with the privileges of the CS-MARS administrator via the optional JBoss JMX console. This vulnerability is documented by Cisco bug ID [CSCse47646](#) ([registered](#) customers only) .
- The CS-MARS CLI is a restricted shell environment which allows authenticated administrators to perform system maintenance tasks. The CLI contains several privilege escalation vulnerabilities which may allow shell commands to be executed on the underlying appliance operating system with root privileges. These vulnerabilities are documented by Cisco bug IDs [CSCsd29111](#) ([registered](#) customers only) , [CSCsd31371](#) ([registered](#) customers only) , [CSCsd31377](#) ([registered](#) customers only) , [CSCsd31392](#) ([registered](#) customers only) and [CSCsd31972](#) ([registered](#) customers only) .

[Top of the section](#) [Close Section](#)

☐ Impact

This section describes the impact of these vulnerabilities.

- Exploitation of the default Oracle accounts vulnerability ([CSCsd16256](#) ([registered](#) customers only)) may result in the compromise of sensitive information contained in the CS-MARS database.
- Exploitation of the JBoss command execution vulnerability ([CSCse47646](#) ([registered](#) customers only)) may allow a remote unauthenticated user to execute arbitrary shell commands with the privileges of the CS-MARS administrator.
- Exploitation of the CLI command execution vulnerabilities ([CSCsd29111](#) ([registered](#) customers only) , [CSCsd31371](#) ([registered](#) customers only) , [CSCsd31377](#) ([registered](#) customers only) , [CSCsd31392](#) ([registered](#) customers only) and [CSCsd31972](#) ([registered](#) customers only)) may allow an authenticated administrator to execute arbitrary shell commands with root privileges.

[Top of the section](#) [Close Section](#)

☐ Software Version and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

CS-MARS versions 4.2.1 and later contain the fixes for all vulnerabilities referenced in this

advisory.

CS-MARS upgrades are incremental. All available updates must be applied in order to reach the most recent version. The upgrade path is documented at:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/3.4/release/notes/rn343.html

CS-MARS software updates can be obtained at the following site:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars?psrtdcat20e2>

[Top of the section](#) [Close Section](#)

☐ **Workarounds**

There are no workarounds for these vulnerabilities.

[Top of the section](#) [Close Section](#)

☐ **Obtaining Fixed Software**

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

[Top of the section](#) [Close Section](#)

☐ **Customers with Service Contracts**

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

[Top of the section](#) [Close Section](#)

☐ **Customers using Third Party Support Organizations**

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

[Top of the section](#) [Close Section](#)

☐ Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

[Top of the section](#) [Close Section](#)

☐ Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

The JBoss vulnerability ([CSCse47646](#) ([registered](#) customers only)) was reported to Cisco by Jon Hart.

[Top of the section](#) [Close Section](#)

☐ Status of this Notice: FINAL

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

☐ Distribution

This advisory is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20060719-mars.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

☐ Revision History

Revision 1.0	2006-July-19	Initial public release.
--------------	--------------	-------------------------

☐ Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

Help us help you.

☐ **Please rate this document.**

☐ Excellent

- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Send

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)