

# [NEWS] Cisco MARS Default Administrative Password

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00040.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 15 Jan 2006 19:17:14 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

## Cisco MARS Default Administrative Password

---

### SUMMARY

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. All CS-MARS appliances ship with a default password set for the undocumented administrative account root".

Successful exploitation of the vulnerability in CS-MARS will result in an attacker gaining full administrative privileges on the CS-MARS device.

### DETAILS

Vulnerable Systems:

- \* CS-MARS version 4.1.2 and prior

Immune Systems:

- \* CS-MARS version 4.1.3

The Cisco Security Monitoring, Analysis and Response System (CS-MARS)

## [NEWS] Cisco MARS Default Administrative Password

software contains a default password for an undocumented administrative account. This password is set, without any user intervention, during installation of the software used by CS-MARS appliances, and is the same in all installations of the product. Users must be authenticated to the CS-MARS command line in order to utilize the default password to access the administrative account.

This privileged account is intended to be used only by authorized Cisco development engineers for advanced debugging purposes. No direct remote access to the root account is permitted. In order to access a privileged system shell, users must first successfully login into the CS-MARS system administration command line interface with the "pnadmin" account. Once authenticated, the root account can be accessed with the undocumented command "expert".

Prior to CS-MARS version 4.1.3, users do not have a method to modify the root password. CS-MARS versions 4.1.3 and later provide the command "passwd expert", which allow users to modify a portion of the root password providing additional security. The selected user password is combined with a Cisco controlled component to form a new root password.

After performing this step, neither Cisco personnel or the user can access the root account without knowledge of both components used to create the root password. When authorized Cisco development engineers need access to the root account for advanced debugging, both Cisco and the user will need to enter their portion of the configured root password to enable access.

### Workaround:

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

```
prompt$ ssh pnadmin@xxxxxxxxxxx
pnadmin@xxxxxxxxxxx's password:
Last login: Fri Dec 30 15:19:14 2005 from 192.168.1.2
```

### CS MARS – Mitigation and Response System

? for list of commands

```
[pnadmin]$ version
4.1.2 (2042)
```

The vulnerability described in this advisory can be mitigated by first upgrading the software on CS-MARS appliances to version 4.1.3 and then using the "passwd expert" command to modify the root password.

CS-MARS appliances can be upgraded via the HTTPS management interface or system administration command line. Please refer to the CS-MARS product documentation for instructions on how to upgrade the software.

While the documentation refers to CS-MARS 4.x versions, the instructions

[NEWS] Cisco MARS Default Administrative Password

are also applicable to CS-MARS 3.x versions.

[http://www.cisco.com/en/US/products/ps6241/products\\_installation\\_guide\\_chapter09186a00804c4db4.html#wp1133](http://www.cisco.com/en/US/products/ps6241/products_installation_guide_chapter09186a00804c4db4.html#wp1133)  
[http://www.cisco.com/en/US/products/ps6241/products\\_installation\\_guide\\_chapter09186a00804c4db4.html#wp1133](http://www.cisco.com/en/US/products/ps6241/products_installation_guide_chapter09186a00804c4db4.html#wp1133)

Once a CS-MARS appliance is upgraded to version 4.1.3, the root password can be modified using the "passwd expert" command. Using a SSH client, login into the CS-MARS system administration interface with the "pnadmin" account and use the "passwd expert" command to select a new password. The selected password must be at least six characters long.

```
prompt$ ssh pnadmin@xxxxxxxxxxx
pnadmin@xxxxxxxxxxx's password: Last
login: Fri Dec 30 19:45:51 2005 from 192.168.1.2
```

CS MARS – Mitigation and Response System

? for list of commands

```
[pnadmin]$ passwd expert
New password:
Retype new password:
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:psirt@xxxxxxxx> Cisco Systems.

The original article can be found at:

<http://www.cisco.com/warp/public/707/cisco-sa-20060111-mars.shtml>  
<http://www.cisco.com/warp/public/707/cisco-sa-20060111-mars.shtml>

=====

This bulletin is sent to members of the SecuriTeam mailing list.  
To unsubscribe from the list, send mail with an empty subject line and body to:  
list-unsubscribe@xxxxxxxxxxxxxxxx  
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind. In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- Prev by Date: [\*\[NT\] Windows Embedded Open Type \(EOT\) Font Heap Overflow\*](#)
- Next by Date: [\*\[TOOL\] IRC DCC Connect\(\) Blind Port Scanner\*](#)
- Previous by thread: [\*\[NT\] Windows Embedded Open Type \(EOT\) Font Heap Overflow\*](#)
- Next by thread: [\*\[TOOL\] IRC DCC Connect\(\) Blind Port Scanner\*](#)
- Index(es):
  - ◆ [\*Date\*](#)
  - ◆ [\*Thread\*](#)