

# Cisco Security Advisory: Default Passwords in the Application Velocity System

Advisory ID: cisco-sa-20080123-avs

<http://www.cisco.com/warp/public/707/cisco-sa-20080123-avs.shtml>

## Revision 1.0

For Public Release 2008 January 23 1600 UTC (GMT)

---

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

---

## Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of this Notice: Final](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

---

# Summary

Versions of the Cisco Application Velocity System (AVS) prior to software version AVS 5.1.0 do not prompt users to modify system account passwords during the initial configuration process. Because there is no requirement to change these credentials during the initial configuration process, an attacker may be able to leverage the accounts that have default credentials, some of which have root privileges, to take full administrative control of the AVS system.

After upgrading to software version AVS 5.1.0, users will be prompted to modify these credentials.

Cisco will make free upgrade software available to address this vulnerability for affected customers. The software upgrade will be applicable only for the AVS 3120, 3180, and 3180A systems. The workaround identified in this document describes how to change the passwords in current releases of software for the AVS 3110.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0029 has been assigned to this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080123-avs.shtml>.

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

## ☐ Affected Products

### ☐ Vulnerable Products

This vulnerability affects the Cisco AVS 3110, 3120, 3180, and 3180A Management Station appliances that are running software versions prior to AVS 5.1.0. Administrators can determine the software version of the AVS appliances by logging in to the Management Station web-based user interface or from the command-line interface (CLI) of the appliance operating system.

Customers who use the AVS 3180 or 3180A Management Station can determine their node software versions by navigating to the [Cluster Information Page](#). Each registered node will display the corresponding software version when the node is selected.

The AVS appliance version can also be determined from the host operating system by using the **Show Version** command.

The following example shows **Show Version** output for an AVS 3120 appliance that is running

version 5.1.0:

```
velocity>Show Version
```

```
*****  
Cisco Application Velocity System,(AVS)  
-----  
AVS 3120-K9 005.001(000.034)  
*****
```

The following example shows **Show Version** output for an AVS 3180 or 3180A appliance that is running version 5.1.0:

```
velocity>Show Version
```

```
*****  
Cisco Application Velocity System,(AVS)  
-----  
AVS 3180-MGMT 005.001(000.034)  
*****
```

## ☐ Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by this vulnerability.

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

## ☐ Details

The Cisco AVS 3110 and 3120 are enterprise data center appliances for improving web application performance, measuring end-user response time, and managing application security. The Cisco AVS 3120 enforces application security with an integrated web application firewall. The Cisco AVS 3180 and 3180A Management Stations provide web-based tools for the configuration and application performance monitoring for a cluster of AVS 3110s and 3120s or individual nodes.

The Cisco AVS 3110, 3120, 3180, and 3180A Management Stations use some system accounts that are initially configured with default passwords. Vulnerable versions of the AVS software do not prompt the administrator to change the passwords for these accounts, including accounts with root privileges, during the initial configuration process. Non-vulnerable versions of AVS software will now prompt administrators to change these accounts after installation.

**Note:** If the passwords for the AVS 3110 or 3120 are changed on the device itself and it has previously been registered with an AVS 3180 or 3180A Management Station, the node must be re-registered with the Management Station console. Otherwise, communication between the AVS 3180 or 3180A Management Station and AVS 3110 or 3120 node will be lost.

For additional details about the AVS node registration process, refer to the Register Node section of the [Cisco AVS User's Guide](#).

After upgrading the appliance software to version AVS 5.1.0 and logging in for the first time, the administrator will now be prompted to change the system account passwords.

The following example shows the new password change prompts and the subsequent password change dialog for the AVS 3120 after upgrade:

```
velocity login: fgn
Password:
**WARNING** System wide secrets are in factory default
state.
Would you like to change these now? [y/n] y changing root
password
enter password:
enter password again:
changing fgn password
enter password:
enter password again:
changing DB password
enter password:
enter password again:

Please wait...The DB password change will take a few
minutes.
changing node manager password
enter password:
enter password again:
changing condenser password
enter password:
enter password again:
changing console password
enter password:
enter password again:
```

The following example shows the new password change prompts and the subsequent password

change dialog for the AVS 3180 and 3180A after upgrade:

```
velocity login: fgn
Password:
**WARNING** System wide secrets are in factory default
state.
Would you like to change these now? [y/n] y changing root
password
enter password:
enter password again:
changing fgn password
enter password:
enter password again:
changing DB password
enter password:
enter password again:
```

Please wait...The DB password change will take a few minutes.

```
changing console password
enter password:
enter password again:
```

This issue is documented in Cisco Bug ID [CSCsd94732](#) ( [registered](#) customers only) .

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

## ☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss>.

<b>CSCsd94732 - AVS Default Account Passwords Don't Require Change.</b>					
<b>Calculate the environmental score of <a href="#">CSCsd94732</a></b>					
<b>CVSS Base Score - 10</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
<b>CVSS Temporal Score - 8.3</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

## [-] Impact

Successful exploitation of the vulnerability may result in full administrative control of the Cisco AVS system or user-level access to the host operating system.

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

## [-] Software Versions 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.

AVS software version 5.1.0 contains the fix for the vulnerability described in this document.

AVS software is available for download from the following locations on cisco.com:

- [AVS 3120 5.1.0](#) ( [registered](#) customers only)
- [AVS 3180 5.1.0](#) ( [registered](#) customers only)

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

## ☐ Workarounds

The following workarounds are applicable only for the AVS 3110 and are performed on the system shell. The AVS 3110 does not have a CLI. The use of strong passwords is encouraged.

### Changing the Root Password

Complete these steps:

1. Change the *root* password by using the following command:

```
shell# passwd
```

2. Reboot to activate the new settings by using the following command:

```
shell# reboot
```

### Changing the Management Console Username and Password

Complete these steps:

1. Open the following file in a text editor:

```
$AVS_HOME/console/jboss-3.0.1_tomcat-4.0.4/server/default/deploy/fgconsole.war/users.  
properties
```

Use the line **admin=admin** to set the username and password. The username appears before the equal sign (=) and the password appears after the equal sign (=). For example, to change the username to *Cisco* and the password to *accelerate*, change the **admin=admin** line to

## Cisco=accelerate.

2. If you change the username, you must also change this file:

```
$AVS_HOME/console/jboss-3.0.1_tomcat-4.0.4/server/default/deploy/fgconsole.war/roles.properties
```

The username is set by the line that contains **admin=**. The username appears before the equal sign (=). For example, to change the user name to *Cisco*, change the **admin=** line to **Cisco=**. Do not change the text after the equal sign (=) in this file; this field specifies the account privileges. The username that you enter here must match the one in the *users.properties* file in the preceding step.

## Changing the Database Username and Password

There are two steps required to change the database password:

1. First change the database password.
2. Then update the Management Console configuration file with the new database password.

Complete these steps:

1. Log in to the database using the old password, and then use the **alter SQL** command to change to the new password.

```
/usr/local/fineground/console/postgres/bin/psql
-U fineground -p 5432 fgnlog
Password : <old password>
Welcome to psql 7.3.4, the PostgreSQL interactive
terminal.
```

```
Type: \copyright for distribution terms
      \h for help with SQL commands
      \? for help on internal slash commands
      \g or terminate with semicolon to execute
query
      \q to quit
fgnlog=# alter user fineground password '<new
password>'; \q
```

2. The username and password to access the Management Console database are set during the Management Console installation process. If you want to change these later, you can modify

an XML configuration file that the Management Console server reads at start-up.

- a. Open the following file in a text editor:

```
$AVS_HOME/console/jboss-3.0.1_tomcat-4.0.4/server/default/deploy/postgres-  
service.xml
```

Look for the following section in this file:

```
<!--set these only if you want only default  
logins,  
                                not through JAAS -->  
<config-property name="UserName" type="java.  
lang.String">fineground</config-property>  
<config-property name="Password" type="java.  
lang.String">condenser</config-property>
```

- b. To change the username, change the value for the UserName configuration property (*fineground* in this example).
- c. To change the password, change the value for the Password configuration property (*condenser* in this example).
- d. Save and close the file.

## Changing the Node Manager Password

Complete these steps:

1. Log in as **fgn**, and then use the **su** command to switch to the superuser.
2. Stop the Condenser and Node Manager:

```
/etc/init.d/fgnnpn<Tab> stop
```

Press **Tab** to have the interface complete the command.

3. Go to the **\$AVS\_HOME/perfnode/node\_manager/conf** directory.
4. Back up the file named *passwords*.

5. Change the password with the following command:

```
$AVS_HOME/perfnode/bin/htpasswd -bcm passwords.new  
admin <password>
```

In the preceding command, *passwords.new* is the name of the file in which the passwords are stored. Currently only the user **admin** is supported.

6. Install the file with the following command:

```
install -m 400 -o nobody -g nobody passwords.new  
passwords
```

7. Restart the appliance with the **reboot** command.

8. Re-register the node from the Management Console for which the node manager password was changed.

## Changing the Condenser Password

Complete these steps:

1. Log in as **fgn**, and then use the **su** command to switch to the superuser.
2. Stop the Condenser and Node Manager:

```
/etc/init.d/fgnnpn<TAB> stop
```

Press **Tab** to have the interface complete the command.

3. Go to the **\$AVS\_HOME/perfnode/passwd** directory.
4. Backup the file named *.htpasswd*.
5. Change the password with the following command:

```
$AVS_HOME/perfnode/bin/htpasswd -bcm passwords.new  
fineground <password>
```

In the preceding command, *passwords.new* is the name of the file in which the passwords are stored. Currently only the user **fineground** is supported.

6. Install the file with the following command:

```
install -m 400 -o nobody -g nobody passwords.new .  
htpasswd
```

7. Restart the appliance with the **reboot** command.

8. Re-register the node from the Management Console for which the Condenser password was changed.

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

## ☐ **Obtaining Fixed Software**

Cisco has released software updates that address this vulnerability. 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/en/US/docs/general/warranty/English/EU1KEN\\_.html](http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html) , or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml> .

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

### **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>.

### **Customers using Third Party Support Organizations**

Customers whose Cisco products are provided or maintained through prior or existing agreements 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.

## Customers without Service Contracts

Customers who purchase direct from Cisco but do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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](mailto:tac@cisco.com)

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

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including 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.

This vulnerability was identified through internal testing.

[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.

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

## ☐ **Distribution**

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

<http://www.cisco.com/warp/public/707/cisco-sa-20080123-avs.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](mailto:cust-security-announce@cisco.com)
- [first-teams@first.org](mailto:first-teams@first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto: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.

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

## ☐ **Revision History**

Revision 1.0	2008-January-23	Initial public release
--------------	-----------------	------------------------

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

## ☐ 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](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>.

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

---

### 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)



[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.](#)