

# Cisco Security Advisory: AVS TCP Relay Vulnerability

Document ID: 70094

Advisory ID: cisco-sa-20060510-avs

<http://www.cisco.com/warp/public/707/cisco-sa-20060510-avs.shtml>

## Revision 1.0

For Public Release 2006 May 10 1600 UTC (GMT)

---

Please provide your feedback on this document.

---

**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 Application Velocity System's (AVS) default configuration allows transparent relay of TCP connections to any reachable destination TCP port if the receiving TCP service can process requests embedded in a HTTP POST method message. This issue does not require a software upgrade and can be mitigated by a configuration command for all affected customers.

Fixed versions of the AVS software have been modified to provide a more secure default configuration.

Cisco has made free software available to address this vulnerability for affected customers installing new AVS Devices. The available workaround must be manually configured to mitigate the impact of this vulnerability for existing AVS devices even if upgrading to a fixed version of software.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20060510-avs.shtml>

## Affected Products

This section provides details on affected products.

## Vulnerable Products

AVS 3110 and 3120 Application Velocity Systems running all software versions prior to 5.0.1 are affected.

- AVS 3110 4.0 and 5.0
- AVS 3120 5.0.0

as well as all prior versions for both devices.

## Products Confirmed Not Vulnerable

The AVS 3180 Management Station is not affected by this vulnerability.

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

## Details

The Cisco AVS 3100 series Application Velocity System is an enterprise appliance for improving application performance. Using the Application Velocity System, web applications deployed across the WAN can offer response times typically expected from LAN environments.

By default, the AVS is normally deployed as a transparent proxy. The transparent proxy feature may be exploited to open a TCP connection to any reachable destination TCP port and hide the true IP source address of the connection TCP port, if the receiving service can process requests embedded in a HTTP POST method message.

This issue has been resolved by changing the default behavior such that connections are limited based on the destination port numbers and connections to TCP ports other than 80 and 443 are denied.

This issue is documented by the following Cisco bug ID:

- CSCsd32143 (registered customers only)

**Note:** The available workaround must be manually configured to mitigate the impact of this vulnerability for existing AVS devices even if upgrading to a fixed version of software.

## Impact

The AVS may be used to forward unexpected traffic and to obscure the true originator of undesirable traffic.

## 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.

This issue is fixed for new installations in AVS version 5.0.1 for both the AVS 3110 and AVS 3120.

Software for AVS 3110 is available at <http://www.cisco.com/cgi-bin/tablebuild.pl/AVS3110-5.0.1>

Software for AVS 3120 is available at <http://www.cisco.com/cgi-bin/tablebuild.pl/AVS3120-5.0.1>

**Note:** The available workaround must be manually configured to mitigate the impact of this vulnerability for existing AVS devices even if upgrading to a fixed version of software.

## Workarounds

For existing AVS devices, this issue must be resolved by a configuration command which blocks the use of redirected proxy requests for any TCP ports other than TCP/80 and TCP/443. To avoid writing over an existing configuration, this command must be manually applied even if software is upgraded to a fixed version. The configuration commands below should be added to the fgn.conf configuration file using the AVS Management Console.

```
<DestinationMapping>  
Name default:80 -> default:80  
Name default:443 -> default:443  
Name default -> localhost:9  
</DestinationMapping>
```

With this Destination map, only TCP connections to ports 80 and 443 will be forwarded. The AVS will reset connections destined to any other ports. If HTTP connections must be completed to other TCP ports, they must also be added to the configuration element using the same syntax as shown above. If destinations are already set in the configuration element, only the

```
Name default -> localhost:9
```

configuration line needs to be added as the last line in the Destination map. Adding this line before other lines in the Destination map may block legitimate traffic. After updating the Destination map element, the configuration changes must be published.

For information on using the AVS Management Console refer to:

[http://www.cisco.com/en/US/products/ps6492/products\\_user\\_guide\\_chapter09186a008059be02.html](http://www.cisco.com/en/US/products/ps6492/products_user_guide_chapter09186a008059be02.html)

For information about the fgn.conf file refer to:

[http://www.cisco.com/en/US/products/ps6492/products\\_user\\_guide\\_chapter09186a008059bddb.html#wp1045951](http://www.cisco.com/en/US/products/ps6492/products_user_guide_chapter09186a008059bddb.html#wp1045951)

For information about Destination Mapping refer to:

[http://www.cisco.com/en/US/products/ps6492/products\\_user\\_guide\\_chapter09186a008059bddb.html#wp1045807](http://www.cisco.com/en/US/products/ps6492/products_user_guide_chapter09186a008059bddb.html#wp1045807)

## 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.

## 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 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.

## 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](mailto: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/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

## Exploitation and Public Announcements

The Cisco PSIRT is aware of an instance in which the AVS has been used to transmit unsolicited commercial e-mail and hide the true source of the message.

## 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-20060510-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.

## Revision History

Revision 1.0	2006-May-10	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](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>.

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Jun 04, 2007

Document ID: 70094

---