

Table of Contents

<u>Cisco Security Advisory: ACNS Denial of Service and Default Admin Password Vulnerabilities</u>	1
<u>Document ID: 64069</u>	1
<u>Revision 1.0</u>	1
<u>For Public Release 2005 February 24 1600 UTC (GMT)</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Affected Products</u>	1
<u>Vulnerable Products</u>	2
<u>Products Confirmed Not Vulnerable</u>	3
<u>Details</u>	3
<u>Impact</u>	3
<u>Software Versions and Fixes</u>	4
<u>Obtaining Fixed Software</u>	5
<u>Customers with Service Contracts</u>	5
<u>Customers using Third-party Support Organizations</u>	5
<u>Customers without Service Contracts</u>	5
<u>Workarounds</u>	6
<u>Exploitation and Public Announcements</u>	7
<u>Status of This Notice: FINAL</u>	7
<u>Distribution</u>	7
<u>Revision History</u>	8
<u>Cisco Security Procedures</u>	8

Cisco Security Advisory: ACNS Denial of Service and Default Admin Password Vulnerabilities

Document ID: 64069

Revision 1.0

For Public Release 2005 February 24 1600 UTC (GMT)

Please provide your feedback on this document.

Summary
Affected Products
Details
Impact
Software Versions and Fixes
Obtaining Fixed Software
Workarounds
Exploitation and Public Announcements
Status of This Notice: FINAL
Distribution
Revision History
Cisco Security Procedures

Summary

Devices running Cisco Application and Content Networking System (ACNS) software may be vulnerable to Denial of Service (DoS) attacks and may contain a default password for the administrative account. Devices running ACNS software may be vulnerable to the DoS attacks while configured as a transparent proxy server, forward proxy server, or reverse proxy server. Cisco has made free software available to address the DoS vulnerabilities for all affected customers. The administrative account default password does not require a software upgrade and can be changed by a configuration command for all affected customers. There are workarounds available to mitigate the effects of two of the vulnerabilities.

The vulnerabilities are documented as the following Cisco Bug IDs:

- **CSCef27476** (registered customers only)
- **CSCef30460** (registered customers only)
- **CSCeg49648** (registered customers only)
- **CSCeg23731** (registered customers only)
- **CSCef30743** (registered customers only)

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050224-acnsdos.shtml>.

Affected Products

Vulnerable Products

DDTS Bug ID	Vulnerable ACNS Versions
CSCef27476	5.0 prior to release 5.0.17.6
	5.1 prior to release 5.1.11.6
CSCef30460	All 4.X releases
	All 5.0 releases
	5.1 prior to release 5.1.11.6
CSCeg49648	All 5.1 releases
CSCeg23731	All 5.0 releases
	5.1 prior to release 5.1.13.7
	5.2 prior to release 5.2.3.9
CSCef30743	All 4.X releases
	All 5.0 releases
	All 5.1 releases
	All 5.2 releases

The hardware models that support ACNS are:

- Cisco 500 Series Content Engines
- Cisco 7300 Series Content Engines
- Cisco Content Routers 4400 series
- Cisco Content Distribution Manager 4600 series
- Cisco Content Engine Module for Cisco 2600, 2800, 3600, 3700, and 3800 series Integrated Service Routers

To determine the ACNS software running on a supported device, log in to the device and issue the **show version** command to display the system banner. Cisco ACNS Software will identify itself as Application and Content Networking System Software (ACNS) . Below the copyright information the ACNS release and build information is displayed.

The following example identifies a Cisco device running ACNS software release 5.1.5.2:

```
Application and Content Networking System Software (ACNS)

Copyright 1999-2003 by Cisco Systems, Inc.

Application and Content Networking System Software Release 5.1.5 (build b2 Mar 30 2004)
```

To match the release and build information from the device with the software release information in this advisory and available on CCO, append the release with the build code and replace the lowercase 'b' with a dot (example: 5.1.5b2 becomes 5.1.5.2)

Products Confirmed Not Vulnerable

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

Details

ACNS software provides web application acceleration and caching services. Cisco ACNS software combines the technologies of demand-pull caching, pre-positioning, and live and on-demand streaming to accelerate delivery of web applications, object files, live events, and video. Bandwidth-intensive content objects, such as Java applets, Flash animations, Shockwave programs, and other file formats can be managed and scheduled for distribution to Content Engines during off-peak hours.

Cisco ACNS software may be vulnerable to four DoS attacks and may contain a default password for the administrative account. Devices running ACNS software may be vulnerable to the DoS attacks while configured as a transparent proxy server, forward proxy server, or reverse proxy server. The issues are detailed below:

- **CSCef27476** — A specifically crafted Transmission Control Protocol (TCP) connection may cause the ACNS cache process to restart resulting in a loss of cached information and degraded service of web browser content requests. Repeated exploitation could result in a sustained DoS attack against the caching functionality of the device.
- **CSCef30460** — Certain malformed IP packets may cause the CPU utilization on the affected device to go to 100% resulting in a degradation of all services. A reboot of the device is required to recover from the high CPU. Repeated exploitation could result in a sustained DoS attack.
- **CSCeg49648** — Certain malformed packets may cause the RealServer RealSubscriber to consume 100% of the affected device's CPU resulting in a degradation of all services. A reboot of the device is required to recover from the high CPU. Repeated exploitation could result in a sustained DoS attack.
- **CSCeg23731** — Certain crafted IP packets may cause the ACNS to continuously forward copies of the crafted packet until all network bandwidth is consumed and network utilization reaches 100%. This could result in a denial of service to the affected device and other devices on the same local network segment with the affected device. A reboot of the device is required to recover from this condition. Repeated exploitation could result in a sustained DoS attack to all devices on the local network segment.
- **CSCef30743** — The administrative password is set to a default password that is the same in all installations if the ACNS setup dialog has not been previously run or the administrative password has not been manually changed. All enabled services will use the default credential.

Impact

- **CSCef27476** — Exploitation of this vulnerability may cause a loss of cached information and degraded service of web browser content requests. Repeated exploitation could result in a sustained DoS attack against the caching functionality of the device.
- **CSCef30460** — Exploitation of this vulnerability may cause a degradation of all services provided by the affected device. Repeated exploitation could result in a sustained DoS attack.
- **CSCeg49648** — Exploitation of this vulnerability may cause a degradation of all services provided by the affected device. Repeated exploitation could result in a sustained DoS attack.
- **CSCeg23731** — Exploitation of this vulnerability may cause a denial of service to the affected device and other devices on the same local network segment. Repeated exploitation could result in a sustained DoS attack.

- **CSCef30743** — An attacker who is able to log into an ACNS device using the default administrative password has full control of the device, which includes the ability to change device configurations.

Software Versions and Fixes

When considering software upgrades, please also consult http://www.cisco.com/en/US/products/products_security_advisories_listing.html 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") for assistance.

DDTS Bug ID	Vulnerable ACNS Versions	Fixed Versions
CSCef27476	5.0 prior to release 5.0.17.6	5.0.17.6 and later
	5.1 prior to release 5.1.11.6	5.1.11.6 and later
CSCef30460	All 4.X releases	Upgrade to 5.1.11.6 and later
	All 5.0 releases	Upgrade to 5.1.11.6 and later
	5.1 prior to release 5.1.11.6	5.1.11.6 and later
CSCeg49648	All 5.1 releases	Upgrade to 5.2.1.7 or later
CSCeg23731	All 5.0 releases	Upgrade to 5.1.13.7 and later or upgrade to 5.2.3.9 and later
	5.1 prior to release 5.1.13.7	5.1.13.7 and later
	5.2 prior to release 5.2.3.9	5.2.3.9 and later
CSCef30743	All 4.X, 5.0, 5.1, and 5.2 releases	Upgrade not required. Implement the workaround detailed in the Workarounds section if necessary

Upgrade procedures can be found in the following documents:

- **Cisco ACNS Software Deployment and Configuration Guide, Release 5.0**
Chapter 10: Upgrading and Downgrading the Software

Note: This procedure includes steps for migrating from 4.X software to ACNS 5.X software

- **Cisco ACNS Software Deployment and Configuration Guide, Release 5.1**
Chapter 15: Upgrading and Downgrading the Software

Note: This procedure includes steps for migrating from 4.X software to ACNS 5.X software

- **Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.2**
Chapter 17: Upgrading and Downgrading the Software

Note: This procedure includes steps for migrating from 4.X software to ACNS 5.X software

Obtaining Fixed Software

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 assistance with the upgrade, which should be free of charge.

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

If you need assistance with the implementation of the workarounds, or have questions on the workarounds, please contact the Cisco TAC.

Please 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.

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

See <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.

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>.

Workarounds

The effectiveness of any workaround 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 is the most appropriate for use in the intended network before it is deployed.

- For Denial of Service vulnerability **CSCeg49648**, RealServer RealSubscriber if it is running. By default the RealServer RealSubscriber is disabled. Disabling RealServer RealSubscriber will prevent the ACNS device from acting as a RealServer streaming media caching subscriber. To verify if the RealServer RealSubscriber is running, use the command **show rtsp server real-subscriber**. The following output shows an enabled RealServer RealSubscriber:

```
cacheengine#show rtsp server

Real Subscriber version: ce7325-9.0.2.855
Real Subscriber enabled
Real Subscriber running
Real Subscriber end user license agreement accepted
Real Subscriber evaluation enabled. Estimated 17 days 21 hours left for evaluation.
Real Subscriber license key not installed
Real Subscriber bandwidth enforced is 522240 kbps
```

To disable the RealServer RealSubscriber, use the command **no rtsp server real-subscriber enable** while in global configuration mode as shown below:

```
cacheengine#configure terminal
cacheengine(config)#no rtsp server real-subscriber enable
cacheengine(config)#exit
```

The following output shows a disabled RealServer RealSubscriber:

```
cacheengine#show rtsp server real-subscriber

Real Subscriber version: ce7325-9.0.2.855
Real Subscriber not enabled
Real Subscriber not running
Real Subscriber end user license agreement accepted
Real Subscriber evaluation enabled. Estimated 17 days 21 hours left for evaluation.
Real Subscriber license key not installed
Real Subscriber bandwidth enforced is 522240 kbps
```

More information about the RealServer RealSubscriber implementation can be found in the Enabling RealSubscriber section of the **Cisco ACNS Software Deployment and Configuration Guide, Release 5.1**.

- For the potential default password issue **CSCef30743**, if the **setup dialog** has been previously run or the administrative password previously changed the workaround is not required. If the **setup dialog** has not been run or the administrative password has not been changed, the workaround is to manually change the **admin** account password. To change the default password, users should run the **username** command once they have logged in as the **admin** user. The following interaction shows an example of a change password dialog on a Content Engine that is performed via the console port:

```
Username: admin
Password:
System Initialization Finished.
Cacheengine#configure terminal
cacheengine(config)#username admin password <password>
```

More information about the username command can be found at:

- ◆ Cisco ACNS 5.2 Software Commands username
- ◆ Cisco ACNS 5.1 Software Commands username
- ◆ Cisco ACNS 5.0 Software Commands username
- ◆ Cisco ACNS 4.2 Software Commands username
- For the Denial of Service vulnerabilities **CSCef27476**, **CSCef30460**, and **CSCeg23731**, access-control lists (ACLs) can be used to reduce exposure to these vulnerabilities. Configure ACLs on the ACNS device and on screening routers, switches and firewalls that filter internal and external traffic to the ACNS device so that IP traffic is only allowed from legitimate, trusted IP addresses.
 - ◆ Refer to <http://www.cisco.com/univercd/cc/td/doc/product/webscale/uce/acns52/ldg52/acls.htm> for information on creating and managing IP access control lists for standalone content engines.
 - ◆ Refer to <http://www.cisco.com/univercd/cc/td/doc/product/webscale/uce/acns52/dcg52/5645acl.htm> for information on creating and managing IP access control lists for centrally managed content engines.
 - ◆ Refer to <http://www.cisco.com/warp/public/707/tacl.html> for examples on how to apply ACLs on Cisco routers.
 - ◆ For more information on anti-spoofing, refer to http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#sec_1 and <http://www.ietf.org/rfc/rfc2827.txt>.
 - ◆ The Unicast Reverse Path Forwarding (Unicast RPF) feature helps to mitigate problems that are caused by spoofed IP source addresses. It is available on Cisco routers and firewalls. For further details, please refer to http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfrpf.htm

Exploitation and Public Announcements

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

Status of This Notice: FINAL

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

A stand-alone copy or paraphrase of the text of this security advisory 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-20050224-acnsdos.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 (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.netsys.com
- 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	2005-February-24	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>.

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Feb 22, 2005

Document ID: 64069
