

Cisco Security Advisory: Multiple Vulnerabilities in the Cisco ACE Application Control Engine Module and Cisco ACE 4710 Application Control Engine

Advisory ID: [cisco-sa-20090225-ace](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20090225-ace.shtml>

Revision 1.1

Last Updated 2009 March 09 2100 UTC (GMT)

For Public Release 2009 February 25 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

The Cisco ACE Application Control Engine Module and Cisco ACE 4710 Application Control Engine Cisco ACE Module and Cisco ACE 4710 Application Control Engine contain multiple vulnerabilities that, if exploited, can result in any of the following impacts:

- Administrative level access via default user names and passwords
- Privilege escalation
- A denial of service (DoS) condition

Cisco has released free software updates available for affected customers. Workarounds that mitigate some of the vulnerabilities are available.

Note: These vulnerabilities are independent of each other. A device may be affected by one vulnerability and not affected by another.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090225-ace.shtml>.

Note: This advisory is being released simultaneously with a multiple vulnerability disclosure advisory that impacts the Cisco 4700 Series Application Control Engine Device Manager and Application Networking Manager module software.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090225-anm.shtml>

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

☐ Affected Products

☐ Vulnerable Products

The following table displays the products that are affected by each vulnerability that is described within this advisory.

Vulnerability	Products and Versions Affected	
	Cisco ACE 4710 Appliance	Cisco ACE Module
Default Usernames and Passwords	All versions prior to A1(8a)	All versions prior to A2 (1.1)
Privilege Escalation Vulnerability	All versions prior to A1(8a)	All versions prior to A2 (1.2)
Crafted SSH Packet Vulnerability	All versions prior to A3(2.1)	All versions prior to A2 (1.3)
Crafted Simple Network Management Protocol version 2 (SNMPv2) Packet Vulnerability	All versions prior to A3(2.1)	All versions prior to A2 (1.3)
Crafted SNMPv3 Packet Vulnerability	All versions prior to A1(8.0)	All versions prior to A2 (1.2)

Determining Software Versions

To display the version of system software that is currently running on Cisco ACE Application Control Engine, use the **show version** command. The following example displays the output of the **show version** command on the Cisco ACE Application Control Engine software version A3 (1.0):

```
ACE-4710/Admin# show version
Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright (c) 1985-2008 by Cisco Systems, Inc. All
rights reserved.
The copyrights to certain works contained herein are
owned by
other third parties and are used and distributed under
```

license.

Some parts of this software are covered under the GNU Public

License. A copy of the license is available at <http://www.gnu.org/licenses/gpl.html>.

Software

```
loader:      Version 0.95
system:      Version A3(1.0) [build 3.0(0)A3(0.0.148)
adbuild_03:31:25-2008/08/06_/auto/adbure_nightly2/
nightly_rel_a3_1_0_throttle/REL_3_0_0_A3_0_0
system image file: (nd)/192.168.65.31/scimitar.bin
```

```
Device Manager version 1.1 (0) 20080805:0415
```

...

<output truncated>

The following example displays the output of the **show version** command on a Cisco ACE Application Control Engine module software version A1(1):

```
ACE-mod/Admin# show version
```

```
Cisco Application Control Software (ACSW)
```

```
TAC support: http://www.cisco.com/tac
```

```
Copyright (c) 2002-2006, Cisco Systems, Inc. All rights reserved.
```

```
The copyrights to certain works contained herein are owned by other third parties and are used and distributed under license.
```

Some parts of this software are covered under the GNU Public

License. A copy of the license is available at <http://www.gnu.org/licenses/gpl.html>.

Software

```
loader:      Version 12.2[117]
system:      Version 3.0(0)A1(1) [build 3.0(0)A1(1)
_01:26:21-2006/03/13_/auto/adbu-rel/ws/REL_3_0_0_A1_1]
```

```
system image file: [LCP] disk0:c6ace-t1k9-mzg.3.0.0_A1_1.bin
```

```
licensed features: no feature license is installed
```

...
<output truncated>

☐ Products Confirmed Not Vulnerable

The Cisco ACE XML Gateway, the Cisco ACE Web Application Firewall, and the Cisco ACE GSS 4400 Series Global Site Selector Appliances are not affected by any of the vulnerabilities that are described in this advisory. No other Cisco products are currently known to be affected by these vulnerabilities.

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

☐ Details

The Cisco ACE 4710 Application Control Engine appliance and the Cisco ACE Application Control Engine Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers are a load-balancing and application-delivery solution for data centers. Multiple vulnerabilities exist in both products. The following information provides the details about each of the vulnerabilities that are addressed in this advisory.

Default Usernames and Passwords

Versions of the Cisco ACE 4710 Application Control Engine appliance prior to software version A1 (8a) use default administrator, web management, and device management account credentials. Similarly, software versions of the Cisco ACE Application Control Engine Module prior to software version A2(1.1) use default administrator and web management credentials. The appliance and module do not prompt users to modify system account passwords during the initial configuration process. An attacker with knowledge of these accounts could modify the application configuration and, in certain instances, gain user access to the host operating system.

This vulnerability is documented in the following Cisco Bug IDs and have been assigned the following Common Vulnerability and Exposures (CVE) IDs:

- Cisco ACE Application Control Engine Module: [CSCsq43828](#) ([registered](#) customers only) - CVE-2009-0620
- Cisco ACE Application Control Engine Appliance: [CSCsq43229](#) ([registered](#) customers only) - CVE-2009-0621

A third account is used for the Cisco 4700 Series Application Control Engine Appliance Device Manager also uses default credentials. Only the Cisco ACE 4710 Application Control Engine appliance is affected by this vulnerability. This vulnerability is documented in Cisco Bug ID

[CSCsq32379](#) ([registered](#) customers only) and has also been assigned the Common Vulnerability and Exposures (CVE) ID CVE-2009-0621.

Privilege Escalation Vulnerability

A vulnerability exists in versions of the Cisco ACE 4710 Application Control Engine appliance prior to A1(8a) and the Cisco ACE Application Control Engine Module prior to version A2(1.2). An authenticated user could exploit this vulnerability to invoke administrative commands via the device command line interface (CLI).

This vulnerability is documented in the following Cisco Bug IDs:

- Cisco ACE Application Control Engine Module: [CSCsq48546](#) ([registered](#) customers only)
- Cisco ACE 4710 Application Control Engine Appliance: [CSCsq09839](#) ([registered](#) customers only)

This vulnerability has been assigned the Common Vulnerability and Exposures (CVE) ID CVE-2009-0622.

Crafted SSH Packet Vulnerability

A vulnerability exists in the Cisco ACE 4710 Application Control Engine appliance prior to software version A3(2.1) and the Cisco ACE Application Control Engine Module prior to software version A2(1.3). An attacker could exploit this vulnerability to cause the device to reload by sending a crafted SSH packet to it.

Note: SSH access must be configured on the affected device for it to be vulnerable. SSH access is not enabled by default. A full TCP three-way handshake is not necessary to trigger the effects of this vulnerability.

This vulnerability is documented in the following Cisco Bug IDs:

- Cisco ACE Application Control Engine Module: [CSCsv01877](#) ([registered](#) customers only)
- Cisco ACE 4710 Application Control Engine Appliance: [CSCsv01738](#) ([registered](#) customers only)

This vulnerability has been assigned the Common Vulnerability and Exposures (CVE) ID CVE-2009-0623.

Crafted SNMPv2c Packet Vulnerability

A vulnerability exists in the Cisco ACE 4710 Application Control Engine appliance prior to software version A3(2.1) and the Cisco ACE Application Control Engine Module prior to software version A2(1.3). An authenticated attacker could send a crafted SNMPv1 packet to an affected device to cause it to reload. Although, this vulnerability is triggered by an SNMPv1 packet, the device must be configured for SNMPv2c.

Note: SNMPv2c must be explicitly configured in an affected device in order to process any SNMPv2c transactions. SNMPv2c is not enabled by default.

This vulnerability is documented in the following Cisco Bug IDs:

- Cisco ACE Application Control Engine Module: [CSCsu36038](#) ([registered](#) customers only)
- Cisco ACE 4710 Application Control Engine Appliance: [CSCsu47876](#) ([registered](#) customers only)

This vulnerability has been assigned the Common Vulnerability and Exposures (CVE) ID CVE-2009-0624.

Crafted SNMPv3 Packet Vulnerability

A vulnerability exists in the Cisco ACE 4710 Application Control Engine appliance prior to software version A1(8.0) and the Cisco ACE Application Control Engine Module prior to software version A2(1.2) where an attacker might cause the device to reload by sending a crafted SNMPv3 packet to it.

Note: SNMPv3 must be explicitly configured in an affected device in order to process any SNMPv3 transactions. SNMPv3 is not enabled by default.

This vulnerability is documented in the following Cisco Bug IDs:

- Cisco ACE Application Control Engine Module: [CSCsq45432](#) ([registered](#) customers only)
- Cisco ACE 4710 Application Control Engine Appliance: [CSCso83126](#) ([registered](#) customers only)

This vulnerability has been assigned the Common Vulnerability and Exposures (CVE) ID CVE-2009-0625.

[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> .

CSCsq43828 and CSCsq43229- Default users and passwords on ACE module and appliance

Calculate the environmental score of [CSCsq43828, CSCsq43229](#)

CVSS Base Score - 10

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete

CVSS Temporal Score - 8.7

Exploitability	Remediation Level	Report Confidence
High	Official-Fix	Confirmed

CSCsq32379 - DM Default Account Credentials

Calculate the environmental score of [CSCsq32379](#)

CVSS Base Score - 10					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - 8.7					
Exploitability		Remediation Level		Report Confidence	
High		Official-Fix		Confirmed	

CSCsq48546 and CSCsq09839 - Privilege escalation issue on ACE Module and ACE Appliance

Calculate the environmental score of [CSCsq48546](#), [CSCsq09839](#)

CVSS Base Score - 9					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	Complete	Complete	Complete
CVSS Temporal Score - 7.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCsv01877 and CSCsv01738 - Crafted SSH packet may cause ACE module or appliance to reload

Calculate the environmental score of [CSCsv01877](#), [CSCsv01738](#)

CVSS Base Score - 7.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - 6.4					

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

CSCsu36038 and CSCsu47876 - Crafted SNMPv2c packet may crash ACE module and appliance

Calculate the environmental score of [CSCsu36038](#), [CSCsu47876](#)

CVSS Base Score - **6.8**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	None	None	Complete

CVSS Temporal Score - **5.6**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

CSCso83126 and CSCsq45432 - Crafted SNMPv3 packet may crash ACE appliance

Calculate the environmental score of [CSCso83126](#), [CSCsq45432](#)

CVSS Base Score - **7.8**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete

CVSS Temporal Score - **6.4**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

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

☐ **Impact**

An attacker with knowledge of the Default Usernames and Passwords Vulnerability accounts could modify the device configuration and, in certain instances, gain user access to the host operating system.

An exploit of the Privilege Escalation Vulnerability could allow an authenticated attacker to execute host operating system administrative commands.

Successful exploitation of the Crafted SSH Packet Vulnerability, Crafted SNMPv2 Packet Vulnerability, and Crafted SNMPv3 Packet Vulnerability may cause a reload of the affected device. Repeated exploitation could result in a sustained DoS condition.

[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.

Each row of the software table (below) describes the earliest possible releases that contain the fix (along with the anticipated date of availability for each, if applicable) are listed in the "First Fixed Release" column of the table. The "Recommended Release" column indicates the releases which have fixes for all the published vulnerabilities at the time of this Advisory. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Releases" column of the table.

Vulnerability	Products and Versions Affected			
	Cisco ACE 4710 Appliance		Cisco ACE Module	
	First Fixed Release	Recommended Release	First Fixed Release	Recommended Release

Default Usernames and Passwords	A1(8a)	A3(2.1)	A2(1.1)	A2(1.3)
Privilege Escalation Vulnerability	A1(8a)	A3(2.1)	A2(1.2)	A2(1.3)
Crafted SSH Packet Vulnerability	A3(2.1)	A3(2.1)	A2(1.3)	A2(1.3)
Crafted SNMPv2 Packet Vulnerability	A3(2.1)	A3(2.1)	A2(1.3)	A2(1.3)
Crafted SNMPv2 Packet Vulnerability	A1(8.0)	A3(2.1)	A2(1.2)	A2(1.3)

Cisco ACE module software can be downloaded from:

<http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=280557289>

Cisco ACE 4710 Application Control Engine appliance software can be downloaded from:

<http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=281222179>

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

☐ Workarounds

This Security Advisory describes multiple distinct vulnerabilities. These vulnerabilities and their respective workarounds are independent of each other.

Default Usernames and Passwords

To change the default administrative password, use the **username** command in configuration mode. The syntax of this command is as follows:

```
username admin [password [0 | 5] {password}]
```

The keywords, arguments, and options are:

admin--Specifies the default administrative user name.

password--(Optional) Keyword that indicates that a password follows.

0--(Optional) Specifies a clear text password.

5--(Optional) Specifies an MD5-hashed strong encryption password.

password--The password in clear text, encrypted text, or MD5 strong encryption, depending on the numbered option (0 or 5) that you enter. Enter a password as an unquoted text string with a maximum of 64 characters.

For example, to create a user named **admin** that uses the clear text password **my_super_secret_88312**, enter the following command:

```
ACE(config)# username admin password 0  
my_super_secret_88312
```

Note: This process can also be followed to change the www user account credentials. The dm user is for accessing the Device Manager GUI and cannot be modified or deleted. The dm user is an internal user required by the Device Manager GUI; it is hidden on the ACE CLI. For more information refer to: http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA3_1_0/configuration/virtualization/guide/config.html

Privilege Escalation Vulnerability

There are no workarounds for this vulnerability.

Crafted SSH Packet Vulnerability

SSH management traffic that can be received by the ACE is controlled through the use of class maps, policy maps, and service policies.

This Management Traffic Service example denies unauthorized SSH packets that are sent to an affected device. In the following example, 192.168.100.1 is considered a trusted source that requires SSH access to the affected device. Care should be taken to allow all required management access to

the affected device. An attacker could exploit this vulnerability using spoofed packets. This workaround cannot provide complete protection against this vulnerability when the attack comes from a trusted source address.

The following example demonstrates how SSH access to the ACE is only allowed from the 192.168.100.1 host:

```
!-- Configure a class to allow SSH from the trusted source
!  
class-map type management match-all Permit_SSH_Class  
  description Allow SSH from trusted sources Class  
  match protocol ssh source-address 192.168.100.1  
  255.255.255.255  
  
!-- Configure a management policy that allows ssh from the  
!--trusted source configured in the above class  
  
policy-map type management first-match Permit_SSH_Policy  
  description Allow SSH from trusted sources Policy  
  class Permit_SSH_Class  
    permit  
  
!-- Apply the management policy globally  
  
service-policy input Permit_SSH_Policy
```

Additional information about "Configuring SSH Management Sessions" is available at:

http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00_A1/configuration/administration/guide/access.html#wp1049450

Additional information about "Configuring Class Maps and Policy Maps" is available at:

http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00_A1/configuration/administration/guide/mapolicy.html



Warning: It is possible to easily spoof the sender's IP address, which may defeat class maps and access control lists (ACLs) that permit communication to the device from trusted IP addresses.

Crafted SNMPv2 and SNMPv3 Packet Vulnerabilities

SNMP management traffic that can be received by the ACE is controlled through the use of class maps, policy maps, and service policies.

This Management Traffic Service example denies unauthorized SNMP packets on UDP port 161 that are sent to an affected device. In the following example, 192.168.100.1 is considered a trusted source that requires SNMP access to the affected device. Care should be taken to allow all required management access to the affected device. An attacker could exploit this vulnerability using spoofed packets. This workaround cannot provide complete protection against this vulnerability when the attack comes from a trusted source address.

```
!-- Configure a class to allow SNMP from the trusted source
!  
class-map type management match-all Permit_SNMP_Class  
description Allow SNMP from trusted sources Class  
  2 match protocol snmp source-address 192.168.100.1  
  255.255.255.255  
  
!  
!-- Configure a management policy that allows snmp from the  
trusted source configured in the above class  
!  
policy-map type management first-match Permit_SNMP_Policy  
  description Allow SNMP from trusted sources Policy  
  class Permit_SNMP_Class  
    permit  
  
!-- Apply the management policy globally  
!  
service-policy input Permit_SNMP_Policy
```

Additional information about "SNMP Management Traffic Services" is available at:

http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00_A1/configuration/administration/guide/snmp.html#wp1034011

Additional information about "Configuring Class Maps and Policy Maps" is available at:

http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00_A1/configuration/administration/guide/mapolicy.html

Additional mitigation techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory:

<http://www.cisco.com/warp/public/707/cisco-amb-20090225-ace.shtml>

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

☐ **Obtaining Fixed Software**

Cisco has released free software updates that address these vulnerabilities. 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, 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

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/en/US/support/tsd_cisco_worldwide_contacts.html 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.

These vulnerabilities were found during 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-20090225-ace.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-bulletins@lists.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.

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

☐ **Revision History**

Revision 1.1	2009-March-09	Clarified information about SNMPv2c packets in the <i>Crafted SNMPv2c Packet Vulnerability</i> section. Revised information about the <i>password</i> argument in the <i>Default Usernames and Passwords</i> section.
Revision 1.0	2009-February-25	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. 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.](#)