

Cisco Security Advisory: DOCSIS Read-Write Community String Enabled in Non-DOCSIS Platforms

Advisory ID: [cisco-sa-20060920-docsis](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20060920-docsis.shtml>

Revision 1.0

For Public Release 2006 September 20 1600 UTC (GMT)

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

Contents

- [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

A vulnerability exists in certain Cisco IOS[®] software release trains running on the Cisco IAD2400 series, 1900 Series Mobile Wireless Edge Routers and Cisco VG224 Analog Phone Gateways. Vulnerable versions may contain a default hard-coded Simple Network Management Protocol (SNMP) community string when SNMP is enabled on the device. The default community string is a result of inadvertently identifying these devices as supporting Data Over Cable Service Interface Specification (DOCSIS) compliant interfaces. The consequence of this error is that an additional read-write community string may be enabled if the device is configured for SNMP management, allowing a knowledgeable attacker the potential to gain privileged access to the device.

Cisco is making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20060920-docsis.shtml>.

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

☐ Affected Products

The following products are affected if they run a vulnerable release of Cisco IOS software with the SNMP server enabled. Any version of Cisco IOS software prior to the versions listed in the Fixed Software section below may be vulnerable.

To determine if the SNMP server is running on your device and the default community string is present, issue the **show snmp community** command while in enable mode at the prompt and look for output similar to:

```
Router#show snmp community

Community name: cable-docsis
Community Index: cisco0
Community SecurityName: cable-docsis
storage-type: read-only active
```

If the SNMP server is disabled on your device, output similar to the following will be returned:

```
Router#show snmp community
%SNMP agent not enabled
```

To determine the software running on a Cisco product, log in to the device and issue the **show version** command to display the system banner. Cisco IOS software will identify itself as "Internetwork Operating System Software" or simply "IOS". On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the IOS release name. Other Cisco devices will not have the **show version** command or will give different output.

The following example identifies a Cisco product running IOS release 12.2(15)MC2 with an installed image name of MWR1900-I-M:

```
Cisco Internetwork Operating System Software
IOS (tm) 1900 Software (MWR1900-I-M), Version 12.2(15)MC2, EARLY DEPLOYME
```

Additional information about Cisco IOS release naming can be found at <http://www.cisco.com/warp/public/620/1.html>.

☐ Vulnerable Products

Cisco devices that may be running with affected Cisco IOS software releases include:

- Cisco IAD2430 Integrated Access Device
- Cisco IAD2431 Integrated Access Device
- Cisco IAD2432 Integrated Access Device
- Cisco VG224 Analog Phone Gateway
- Cisco MWR 1900 Mobile Wireless Edge Router

- Cisco MWR 1941 Mobile Wireless Edge Router

☐ Products Confirmed Not Vulnerable


These products are not vulnerable:

- Cisco IAD2420 Integrated Access Device
- Cisco IAD2421 Integrated Access Device
- Cisco IAD2423 Integrated Access Device
- Cisco IAD2424 Integrated Access Device

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

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

☐ Details

Implementation of the Data Over Cable Service Interface Specification (DOCSIS) standards allow for data transmission over physical media used by cable television providers. Accordingly, [RFC 2669](#)  defines the DOCSIS Cable Device MIB, better known as the DOCS-CABLE-DEVICE-MIB, for which support is required in order to be considered DOCSIS compliant. That MIB defines the table, docsDevNmAccessTable, as:

```
"This table controls access to SNMP objects by network management stations. If the table is empty, access to SNMP objects is unrestricted. This table exists only on SNMPv1 or v2c agents and does not exist on SNMPv3 agents. See the conformance section for details. Specifically, for v3 agents, the appropriate MIBs and security models apply in lieu of this table."
```

In order to comply with the DOCSIS standard and to avoid unrestricted access to SNMP objects, Cisco devices which support DOCSIS contain a read-write community string, "cable-docsis".

Inclusion of this SNMP community string is intended only for DOCSIS-compliant cable-capable devices. A vulnerability exists in the inadvertent enabling of this community string in Cisco IOS release trains running on the affected platforms.

Customers running vulnerable versions of Cisco IOS software on those platforms may be unaware of the additional read-write community string.

This vulnerability is documented in Cisco Bug ID [CSCsb04965](#) ([registered](#) customers only) on the Cisco IAD2400 series and Cisco VG224 Analog Phone Gateways and as [CSCsb06658](#) ([registered](#) customers only) on the 1900 Series Mobile Wireless Edge Routers.

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

☐ Impact

Successful exploitation of the vulnerability may result in full control of the device.

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

☐ 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.

Each row of the Cisco IOS software table (below) describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. 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. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

For more information on the terms "Rebuild" and "Maintenance," consult the following URL: <http://www.cisco.com/warp/public/620/1.html>.

Major Release	Availability of Repaired Releases	
Affected 12.2-Based Release	Rebuild	Maintenance
12.2MC	12.2(15) MC2c	
12.2ZJ	Vulnerable; migrate to 12.3(4)T13 or later	
Affected 12.3-Based Release	Rebuild	Maintenance
12.3T	12.3(4) T13	
	12.3(7) T11	
	12.3(8) T10	
	12.3(11) T6	
	Vulnerable; for 12.3 (14), migrate to 12.4 (1b) or later	
12.3XD	Vulnerable; migrate to 12.3(7)T11 or later	
12.3XX	Vulnerable; migrate to 12.4(1b) or later	
12.3XY	Vulnerable; migrate to 12.4(1b) or later	
	Vulnerable; contact	

12.3YA	TAC	
12.3YD	Vulnerable; migrate to 12.4(2)T5 or later	
12.3YF	Vulnerable; migrate to 12.3(14)YX or later	
12.3YG	12.3(14) YG5	
12.3YH	Vulnerable; migrate to 12.4(2)T5 or later	
12.3YI	Vulnerable; migrate to 12.4(2)T5 or later	
12.3YJ	Vulnerable; migrate to 12.3(14)YQ8 or later	
12.3YK	Vulnerable; migrate to 12.4(4)T or later	
12.3YM	12.3(14) YM8	
12.3YQ	12.3(14) YQ8	
12.3YS	Vulnerable; migrate to 12.4(4)T or later	
12.3YT	Vulnerable; migrate to 12.4(4)T or later	
12.3YU	Vulnerable; migrate to 12.4(2)XB or later	
Affected 12.4-Based Release	Rebuild	Maintenance
12.4	12.4(1b)	12.4(3)
12.4MR		12.4(4)MR
12.4T	12.4(2) T5	12.4(4)T

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

☐ Workarounds

The effectiveness of any workarounds 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.

The following workarounds should only be considered as a long term solution if anti-spoofing methods consistently prevent spoofed source attacks from entering the network and access-lists provided below are configured on every potentially affected device.

Disable the SNMP Server

If the SNMP server is not used for any legitimate purposes on the device, it is a best practice to disable it by issuing the following commands in configure mode:

```
no snmp-server
```

Removing the public community string with the configure command **no snmp-server community <string> ro** is not sufficient as the SNMP server will still be running and the device will be vulnerable. The command **no snmp-server** must be used instead. The SNMP server status may be verified by using the enable command **show snmp**. You should see a response of "%SNMP agent not enabled".

Note that this workaround may only be viable if SNMP is not used in any way for managing the device.

Restrict Access via a Community-map

The ability to create a community-map was introduced in Cisco IOS versions 12.0(23)S, 12.2(25)S and 12.3(2)T. This feature adds the ability to create a mapping between an SNMP community and an SNMP context, Engine ID, or security name that is different from the default settings.

When an SNMP community is associated with an SNMP context, whenever a request is made from this community, it is applied to the context specified. This feature can also be used to specify the source address validation for an SNMP community.

Consider the following example:

```
Router(config)#access-list 65 remark Deny access to community string
Router(config)#access-list 65 deny any
Router(config)#snmp-server community no-access RO 65
Router(config)#snmp mib community-map cable-docsis security-name no-acce
```

The above creates a new community named "no-access". The authorization to use the community "no-access" is controlled by an access-list, which in this case denies all hosts from using it. With the addition of the **snmp mib community-map** command, the current community string of "cable-docsis" is then under the access restrictions of the new community string "no-access" preventing any use of the "cable-docsis" community string.

Control Plane Policing

Cisco IOS release trains 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support Control Plane Policing (CoPP) which may be configured to protect the device from attacks that target the management and control planes. The following example can be adapted to your network. This example assumes that all SNMP access is to be restricted to a management station with the IP address of 10.1.1.1, and that the management station need only communicate with router's IP address 192.168.10.1:

```
access-list 111 deny udp host 10.1.1.1 host 192.168.10.1 eq snmp
access-list 111 permit udp any any eq snmp
access-list 111 deny ip any any
!
class-map match-all drop-snmp-class
 match access-group 111
!
```

```

!
policy-map drop-snmp-policy
  class drop-snmp-class
    drop
!
control-plane
  service-policy input drop-snmp-policy

```

Please note that in the 12.0S, 12.2S, and 12.2SX Cisco IOS trains the policy-map syntax is different:

```

policy-map drop-snmp-policy
  class drop-snmp-class
    police 32000 1500 1500 conform-action drop exceed-action drop

```

In the above CoPP examples the ACL entries that match the exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action are not affected by the policy-map drop function.

Additional information on the configuration and use of the CoPP feature can be found at the following URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

Restrict Access to Trusted Hosts Only

Access Control Lists (ACLs) can be used to deny traffic to the device. Although Cisco IOS devices have community-string access lists which check the source address of SNMP requests per community string, they will not work in this case as the cable-docsis community string is not able to be modified or deleted via configuration options.

It is possible to permit UDP traffic to the router from trusted IP addresses with interface ACLs.

Note: Because SNMP is based on UDP, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses.

The following extended access-list can be adapted to your network. This example assumes that the router has IP addresses 192.168.10.1 and 172.16.1.1 configured on its interfaces, that all SNMP access is to be restricted to a management station with the IP address of 10.1.1.1, and that the management station need only communicate with IP address 192.168.10.1:

```

access-list 101 permit udp host 10.1.1.1 host 192.168.10.1 eq snmp
access-list 101 deny udp any host 192.168.10.1 eq snmp
access-list 101 deny udp any host 172.16.1.1 eq snmp
access-list 101 permit ip any any

```

The access-list must then be applied to all interfaces using the following configuration commands:

```

interface FastEthernet 0/0
ip access-group 101 in

```

Note that UDP traffic to port 161 (SNMP) must be explicitly blocked to each IP address on the router to prevent the router from accepting and processing the SNMP packets. Blocking traffic to port 161 from unknown hosts is considered a best practice. All devices that need to communicate directly with the router on port 161 will need to be specifically listed in the above access list.

For devices that have many IP addresses configured, or many hosts that need to communicate with the router, this may not be a scalable solution.

Infrastructure ACLs (iACL)

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for iACLs:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

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

☐ 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.

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

☐ 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>.

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

☐ 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.

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

☐ 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

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.

[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 reported to Cisco by a customer.

[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-20060920-docsis.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
- 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 1.0	2006-September-20	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.](#)