

Cisco Security Advisory: Malformed SNMP Message-Handling Vulnerabilities for Cisco Non-IOS Products

Document ID: 19296

Advisory ID: cisco-sa-20020211-snmp-msgs-non-ios

<http://www.cisco.com/warp/public/707/cisco-sa-20020211-snmp-msgs-non-ios.shtml>

Revision 2.6

Last updated 2004 March 01 0800 UTC (GMT)

For Public Release 2002 February 11 2300 UTC (GMT)

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

[Summary](#)

[Affected Products](#)

[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

Multiple Cisco products contain vulnerabilities in the processing of Simple Network Management Protocol (SNMP) messages. These vulnerabilities can be repeatedly exploited to produce a denial of service. In most cases, workarounds are available that may mitigate the impact. Some of these vulnerabilities are identified by various groups as VU#617947, VU#107186, OUSPG #0100, CAN-2002-0012, and CAN-2002-0013.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20020211-snmp-msgs-non-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that do not run Cisco IOS software.

A companion document describes this vulnerability for products that run Cisco IOS Software,

<http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

To determine if a product is vulnerable, review the list below. If the software versions or configuration information are provided, then only those combinations are vulnerable.

- Catalyst 290x, 292x, 2948g, 3000, 3200, 3900, 4000, 4912g, 5000 series switches
- Catalyst 6000 Supervisor Module, Catalyst 6000 Network Analysis Module (NAM)
- MicroHub 1500, MicroSwitch 1538/1548
- BPX, IGX, MGX WAN switches, and the Service Expansion Shelf
- WAN Manager
- Cisco Secure PIX firewall
- CallManager (if Microsoft SNMP is enabled)
- Unity Server (if Microsoft SNMP is enabled)
- Cisco Secure Intrusion Detection System (NetRanger) appliance and IDS Module
- BR340, WGB340, AP340, AP350, BR350 Cisco/Aironet wireless products
- CSS11000 (Arrowpoint) Content Services Switch
- Content Engine 507, 560, 590, and 7320 running 3.1, 4.0.1, or 4.0.3
- Content Router 4430 and Content Delivery Manager 4630 and 4650 running 4.0
- LocalDirector
- Internet CDN Content Engine 590 and 7320, Content Distribution Manager 4670, and Content Router 4450 running ICDN software 1.0, 2.0, 2.1.0
- VPN3000 (Altiga) VPN Concentrator
- Access Registrar (using Solaris SNMP)
- Cisco ws-x6608 and ws-x6624 IP Telephony Modules
- Traffic Director
- Cisco Info Center
- Switch Probe
- CiscoWorks Windows
- Hosting Solution Engine
- User Registration Tool VLAN Policy Server
- Cisco Element Management Framework
- Cisco Intelligent Contact Management
- Cisco ONS 15454 Optical Transport Platform
- Cisco ONS 15327 Metro Edge Optical Transport Platform
- VG248 Analog Phone Gateway
- Cisco 8110 Broadband Network Termination Unit
- Cisco FastHub 400

Products Confirmed Not Vulnerable

The following Cisco products are not affected by this vulnerability either because they are not vulnerable or because they do not support SNMP. If the software versions or configuration information are provided, then only those combinations are not vulnerable.

- Catalyst 1900, 2820 series switches
- Catalyst 1400 FDDI concentrators
- FastHub 300 Ethernet repeater
- Cache Engine 505 and 570 running versions 2.3 or 2.5
- Content Engine 507, 560 and 590 running versions 2.3 or 2.5
- Content Engine 507 and 560, Content Router 4430 and Content Delivery Manager 4630 and 4650 running E-CDN 3.0.x
- CR-4430-B running Content Router software
- IP/TV

- Device Fault Manager
- ME1100 series
- Voice Manager
- RTM
- IP Phone (all models)
- SN5400 series storage routers
- VPN5000 VPN Concentrator
- Cisco ONS 15190/15194 IP Transport Concentrator
- Cisco ONS 15800/15801/15808 Dense Wave Division Multiplexing Platform
- Cisco ONS 15830 T30 Optical Amplification System
- Cisco ONS 15531/15532 T31 OMDS Metro WDM System
- Cisco ONS 15831/15832 T31 DWDM System
- Cisco ONS 15863 T31 Submarine WDM System

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

Details

SNMP defines a standard mechanism for remote management and monitoring of devices in an Internet Protocol (IP) network.

There are three general types of SNMP operations: "get" requests to request information, "set" requests which modify the configuration of the remote device, and "trap" messages which provide a monitoring function. SNMP requests and traps are transported over User Datagram Protocol (UDP) and are received at the assigned destination port numbers 161 and 162, respectively.

The largest group of vulnerabilities described in this advisory result from insufficient checking of SNMP messages as they are received and processed by an affected system. Malformed SNMP messages received by affected systems can cause various parsing and processing functions to fail, which may result in a system crash and reload (or reboot) in most circumstances. Some Cisco products may not reload but will become unresponsive instead. Some of the affected products are not directly vulnerable to malformed SNMP messages, but fail under extended testing or large volumes of SNMP messages due to memory leaks or other unrelated problems.

These vulnerabilities can be easily and repeatedly demonstrated with the use of the University of Oulu Secure Programming Group (OUSPG) "PROTOS" Test Suite for SNMPv1. The test suite is generally used to analyze a protocol and produce messages that probe various design limits within an implementation of a protocol. Test packets containing overly-long or malformed object identifiers and other combinations of exceptional values in various fields can be programmatically generated and then transmitted to a network device under test. The PROTOS test suite for SNMPv1, as distributed, contains approximately 53,000 individual test cases.

Although the test suite itself applies only to SNMPv1, similar vulnerabilities likely exist in SNMPv2c and SNMPv3. Cisco has attempted to resolve those additional potential vulnerabilities simultaneously.

Independent security advisories have implicated TCP or UDP port 1993 in this vulnerability. Port 1993 is assigned to Cisco for SNMP over TCP, but it appears only in Cisco IOS Software releases prior to 11.x. It is not currently supported nor employed in any current Cisco products.

Impact

The vulnerabilities can be exploited to produce a Denial of Service (DoS) attack. When the vulnerabilities are exploited, they can cause an affected Cisco product to crash and reload.

SNMP messages are transported using User Datagram Protocol (UDP) and are subject to IP source address spoofing which could be used to circumvent the access control mechanisms.

If an attacker is able to guess or otherwise obtain a read-only community string for an affected device, then he or she could bypass SNMP access control relying on the community string.

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.

Cisco Software – IOS

Please review the information in the following link for details on Cisco non-IOS products:

<http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml>

Cisco Software – Non IOS

Each row of the software table (below) describes a product platform set, and the first available fixed release.

In all cases, customers should exercise caution to confirm that the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new software release. If the information is not clear, contact the Cisco TAC for assistance as shown in the [Obtaining Fixed Software](#) section.

This information will be updated as more releases become available.

CatOS Product	Defect ID	Availability of Fixed Releases
Catalyst 4000, Catalyst 5000, Catalyst 6000 Family	CSCdw67458	7.1(2), 7.1(1a), 6.3(5), 6.3(4a), 6.3(3a), 6.3(2a), 6.3(1a), 6.3(3)X1, 6.2(3a), 6.2(2a), 6.2(1a), 6.1(4b), 6.1(3a), 6.1(2a), 6.1(1e), 5.5(13a), 5.5(12a), 5.5(11a), 5.5(10a), 5.5(7a), 5.4(4a), 5.4(2a), 5.3(6a)CSX, 5.2(7a), 5.2(3a)CSX, 5.1(2b), 5.1(1a)CSX, 4.5(13a), 4.5(12a), 4.5(6a)

Each row of the software table (below) describes a product and the defect identifier, and if available, the first fixed release.

In all cases, customers should exercise caution to confirm that the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new software release. If the information is not clear, contact the Cisco TAC for assistance as shown in the [Obtaining Fixed Software](#) section.

This information will be updated as more releases become available.

Product	Defect ID	Intended First Fixed Releases*
Content Networking		
Arrowpoint CS11000	CSCdw64236	4.01.053s, 5.00.037s, 5.01.013s, 5.02.005s
Cache Engine 505/570 Content 507/560/590/7320	CSCdw65996	
Internet CDN	CSCdw69634	2.1.1
Local Director	CSCdw64918	4.2.4
Desktop Switching		
MicroHub 1500	CSCdw70302	1.00.01
Catalyst 3900 Series	CSCdw71510	Not Scheduled
FastHub 400	CSCdw70302	1.00.01
MicroSwitch 1548	CSCdx11736	1.00.08
Consumer DSL		
CBOS	CSCdw65068	2.4.4
IAD 8110	CSCdw73044	6.1
Network Management		
Cat6k NAM	CSCdw61011	1.2(3), 2.1(2)
CiscoWorks Windows/WUG	CSCdw64558	6.03
Hosting Solution Engine	CSCdw60969	1.3.1
SNMPc	CSCdw64713	No fix planned, migrate to CiscoWorks Windows
Switch Probe	CSCdw62257	5.1(b173)
Traffic Director	CSCdw64528	
User Registration Tool – VLAN Policy Server	CSCdw61176	2.0.7
Access Registrar	CSCdw35595	1.7r3
Cisco Info Center	CSCdw62590	3.4.1
Building Broadband Service Manager	CSCdw73222	BBSM SP3

Cisco Element Management Framework (CEMF)	CSCdw62991	CEMF 3.0.4 P14.6-1, CEMF 3.0.4 P15.2-1, CEMF 3.1 P4.4-1, CEMF 3.1 P5.4-2
Voice Products		
Cisco CallManager	CSCdw73686	Apply MS02-006 patch.
Cisco ICS-7750	CSCdw73454	2.2.0
Cisco Intelligent Contact Management	CSCma13657	Apply MS02-006 patch.
WS-X6608	CSCdw62862	003.002(000.147)
WS-X6624	CSCdw62863	003.002(000.147)
BTS10200	CSCdw74207	2.1, 3.2
SC2200/VSC3000	CSCdw72273	
VG248 Analog Phone Gateway	CSCuk32665	1.2 (April 2002)
Carrier Class Products		
BPX/IGX	CSCdw58704	9.1.30, 9.2.41, 9.3.36
Cisco WAN Manager	CSCdw69753, CSCdw69736, CSCdw69954	10.4.10 Patch 2.1, 10.5.10 Patch 1
MGX-8220	CSCdw63646	4.1.12, 5.0.18
MGX-8230, MGX-8250, MGX-8850 R1	CSCdw56886	1.1.27, 1.1.32a, 1.1.35, 1.1.42,
MGX-8850 R2	CSCdw56907	1.2.01, 2.0.16, 2.1.75
Service Expansion Shelf	CSCdw56907	1.0.16, 1.1.75
MGX-8240	CSCdw71793, CSCdw71906	
MGX-8260	CSCdw71474	Not Scheduled
Wireless Products		
AP340 Series, AP352	CSCdw63011	11.05a, 11.06a, 11.07a, 11.08T1, 11.10T1
AP352	CSCdw63031	11.05a, 11.06a, 11.07a, 11.08T1, 11.10T1
BR340 Series, BR352	CSCdw63248	8.24_2, 8.55_2, 8.65_2

BR352	CSCdw63032	11.05a, 11.06a, 11.07a, 11.08T1, 11.10T1
WGB340 Series	CSCdw63264	8.24_2, 8.55_2, 8.65_2
WGB352	CSCdw63264	8.55_2, 8.65_2
Security Products		
NetRanger	CSCdw44477	03.0(04)S16
NetRanger Sensor	CSCdw47000	
PIX	CSCdw63021, CSCdw75833	4.4(9), 5.2(8), 5.3(4), 6.0(3), 6.1(3) (available 2002-02-28)
VPN 3000	CSCdw64623	3.5(2)REL
Optical Products		
ONS 15454	CSCdw73962, CSCdw73976, CSCdw73979, CSCdw73980, CSCdw73983, CSCdw73989 CSCdw75755	2.3(3), 3.2(1), 3.3(0), 3.4(0)

Workarounds

Workarounds are described in this section.

CAT OS

Apply IP Permit List for SNMP to enable access to the switch's management interface only from the network management workstations. For instructions on how to do this, please refer to http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_6_3/config/ip_perm.htm.

Please note that this will not prevent spoofed IP packets with the source IP address set to that of the network management station from reaching the switch's management interface.

Configuration Notes

The following command enables an ip permit list based on SNMP:

```
set ip permit enable snmp
```

The following command enables a specific IP addresses to have SNMP access:

```
set ip permit 192.168.0.100 255.255.255.255 snmp
```

In CatOS versions prior to 5.4(1), IP permit lists based on port number are not supported.

The following command enables an IP permit list that affects both Telnet and SNMP access:

```
set ip permit enable
```

or

```
set ip permit 192.168.0.100 255.255.255.255
```

On the Catalyst 6000 series switches, if the Virtual LAN (VLAN) Access Control List (ACL) (VACL) feature is available in the code base, you can use VACLs instead of the IP Permit List workaround above. For instructions on how to do this, please refer to http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/6.x/configuration/guide/acc_list.html.

Please note that this will not prevent spoofed IP packets with the source IP address set to that of the network management station from reaching the switch's management interface.

PIX

General Information

- SNMP on the PIX is DISABLED by default, and warning messages are displayed to the administrator when SNMP is configured to listen on the OUTSIDE interface.
- SNMP is enabled on the PIX when the Firewall administrator enters the **snmp-server ...** command.
- The PIX is not vulnerable if the PROTO test suite is run from a server whose IP address is not explicitly defined in the **snmp-server host** command. The results of current testing show that the PIX is only vulnerable if SNMP data is received from a host defined in the **snmp-server host ...** command.

Please review the configuration of your PIX and make sure that each of the IP addresses listed in the **snmp-server host ...** command is a legitimate SNMP host. Customers should review configuration for lines such as the following: **snmp-server host outside ip-address** which would permit SNMP queries from the unprotected interface. If they find these commands in the configuration, they should carefully evaluate the necessity for them and the protection offered by other devices upstream to ensure that spoofing of the SNMP host cannot take place.

Best Practices

- Firewall Administrators should evaluate their site security policy and consider implementing SNMP egress filtering (deny UDP port 161 and 162 and TCP and UDP ports 1993) on the PIX Firewall. If your organization does not manage any device that is not on your network, you may want to consider blocking SNMP at your Internet Firewall so that future SNMP exploits cannot be launched from your network.
- Change the **snmp-server** community string to something else other than "public".

```
snmp-server community somethingotherthanpublic
```

Workarounds

- Disable SNMP. You can do this by removing all **snmp-server host** commands.
 - ◆ **no snmp-server host inside ip-address**
 - ◆ **no snmp-server host inside ip-address**

- ◆ `no snmp-server location`
- ◆ `no snmp-server contact`
- ◆ `no snmp-server community public`
- ◆ `no snmp-server enable traps`

Note: Other PIX SNMP commands including the `snmp-server community` may still appear in the PIX configuration after the `no snmp-server host ...` command has been executed.

LocalDirector

General Information:

- SNMP on the LocalDirector is DISABLED by default. There is no "inside/outside" interface as there is on a PIX and therefore no warnings are displayed when SNMP is enabled.
- SNMP is enabled on the LocalDirector when the administrator enters the `snmp-server ...` command.
- The LocalDirector is not vulnerable if malformed SNMP messages are transmitted from a server whose IP address is not explicitly defined in the "snmp-server host" command. The results of current testing show that the LocalDirector is only vulnerable if SNMP data is received from a host defined in the `snmp-server host ...` command. Please review the configuration of your LocalDirector and make sure that each of the IP addresses listed in the `snmp-server host ...` command is an authorized SNMP host. If you find these commands in the config, you should carefully evaluate the necessity for them and the protection offered by other devices upstream to ensure that spoofing of the source address of the SNMP host cannot take place.

Best Practices:

- Change the `snmp-server community` string to something else other than "public".

```
snmp-server community somethingotherthanpublic
```

Workarounds:

- Disable SNMP, you can do this by removing all "snmp-server host" commands.
 - ◆ `no snmp-server host ip-address`
 - ◆ `no snmp-server location`
 - ◆ `no snmp-server contact`
 - ◆ `no snmp-server community public`
 - ◆ `no snmp-server enable traps`

Note: Other LocalDirector SNMP commands including `snmp-server community` may still appear in the LocalDirector configuration after the `no snmp-server host ...` command has been executed.

ArrowPoint/CSS11000

`snmp community public read-write` is the command that is vulnerable to the suite.

By issuing the `show run global` command, you can search for "read-write" to determine if the CSS is vulnerable.

Configure STRONG community string for read–write, and use access lists on the box for additional control.

Cisco Cache Engine

Disable SNMP with the following command:

```
no snmp-server host
```

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. 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

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

Cisco is not aware of any malicious exploitation of this vulnerability.

The largest set of these vulnerabilities were reported by the OUSPG at the University of Oulu, Finland, in concert with the CERT Coordination Center. A small number were reported by Cisco customers and some were internally discovered.

These vulnerabilities are present in other products not provided by Cisco, and this security advisory is being published simultaneously with announcements from the other affected organizations.

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 notice will be posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20020211-snmp-msgs-non-ios.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
- bugtraq@securityfocus.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- firewalls@lists.gnac.com
- Various internal Cisco mailing lists

Future updates of this notice, if any, will be placed on Cisco's Worldwide Web server, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the URL given above for any updates.

Revision History

Revision	2004-Mar-01	Updates made to Software Versions
----------	-------------	-----------------------------------

2.6		and Fixes table Voice Products section.
Revision 2.5	2003-Jan-24	Updates made to software versions and fixes, status changed to Final.
Revision 2.4	2002-Apr-02	Updates made to Software Versions and Fixes.
Revision 2.3	2002-Apr-01	Updates made to Affected Products, and Software Versions and Fixes.
Revision 2.2	2002-Mar-13	Updates made to Affected Products.
Revision 2.1	2002-Mar-08	Updates made to Affected Products, and Software Versions and Fixes.
Revision 2.0	2002-Feb-25	Non- IOS products now a separate advisory, updates to Software Versions and Fixes, and Workarounds.
Revision 1.3	2002-Feb-20	Updates made to the following sections: Software Versions and Fixes, and Workarounds – LocalDirector
Revision 1.2	2002-Feb-16	Updates made to the following sections: Summary, Software Versions and Fixes, Workarounds
Revision 1.1	2002-Feb-13	Table updates
Revision 1.0	2002-Feb-12	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 Web site 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>.

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Mar 01, 2004

Document ID: 19296
