

Cisco Security Advisory: Malformed SNMP Message-Handling Vulnerabilities

Document ID: 19294

Advisory ID: cisco-sa-20020212-snmplib-msgs

<http://www.cisco.com/warp/public/707/cisco-sa-20020212-snmplib-msgs.shtml>

Revision 2.2

Last Updated 2003 December 23 0800 UTC (GMT)

For Public Release 2002 February 12 2000 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. The vulnerabilities can be repeatedly exploited to produce a denial of service. In most cases, workarounds are available that may mitigate the impact. 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-20020212-snmplib-msgs.shtml>.

This advisory only applies to Cisco products that run Cisco IOS Software. A companion document describes this vulnerability as it applies to Cisco products that do not run Cisco IOS Software,

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

Affected Products

This section provides details on affected products.

Vulnerable Products

This security advisory applies to the broad range of Cisco products that run Cisco IOS Software.

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 12.0(3) with an installed image name of C2500-IS-L:

```
Cisco Internetwork Operating System Software IOS (TM)
2500 Software (C2500-IS-L), Version 12.0(3), RELEASE SOFTWARE
```

The release train label is "12.0".

The next example shows a product running IOS release 12.0(2a)T1 with an image name of C2600-JS-MZ:

```
Cisco Internetwork Operating System Software IOS (tm)
C2600 Software (C2600-JS-MZ), Version 12.0(2a)T1, RELEASE SOFTWARE (fc1)
```

Additional information about Cisco IOS Banners is available at <http://www.cisco.com/warp/public/620/1.html#3>.

To determine if a product is vulnerable, review the list below. If software versions or configuration information is included, then only those combinations are affected (or unaffected). If the product or series is listed without any qualifying software version information, then consult the Software Versions and Fixes section to determine if the product is running an affected version of software.

Note: Catalyst switches can be configured to run either IOS or CatOS. Only Catalyst switches that run IOS are described in this document. Catalyst switches running CatOS are covered in the companion non-IOS security advisory at <http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-non-ios-pub.shtml>.

The following Cisco products are vulnerable if they are running an affected version of Cisco IOS Software:

- Cisco 800, 1000, 1400, 1600, 1700, 2000, 2500, 2600, 3011, 3200, 3600, MC3810, 4000, 4500, 4700, 6400-NRP, 6400-NSP series routers
- Cisco 6000 series IP DSL switches
- uBR900 series cable access routers
- CVA120 series cable voice adapters
- IAD2400 series Integrated Access Devices
- Catalyst 2900XL, 2950, 3500XL, 3550, 4000, 4840G, 4908G-L3 series switches
- Cisco AS5000 series access servers
- Catalyst 6000 MSM, 6000 MSFC & MSFC2, 6000 Hybrid Mode, 6000 Native Mode, 6000 Supervisor modules
- Cisco RSM, RSFC, 7000, 7010, 7100, 7200, uBR7200, 7300, 7400, 7500, 7600, uBR10000, 10700, 10000 ESR, and 12000 series routers
- Lightstream 1010 ATM switches
- DistributedDirector 2500 and 4700 series \
- Catalyst 8510CSR, 8510MSR, 8540CSR, 8540MSR series switches

- Cisco ONS 15540 Optical Transport Platform
- Cisco ONS 15303/15304
- Cisco ISR 3303
- Cisco OSR 7609
- Cisco SOHO-70 Small Office/Home Office router
- Cisco AGS, AGS+, CGS, IGS, MGS series routers
- Cisco 1000 series LAN Extender
- Cisco AccessPro PC card router
- Cisco 200, ASM-CS, and 500-CS series access servers
- Cisco 2500 FRAD series router
- 3011 WAN module for the Catalyst 3200 switch
- Cisco AccessPath TS-3 system shelf

Products Confirmed Not Vulnerable

This vulnerability potentially affects all major software release trains for Cisco IOS Software. Therefore, any Cisco product that runs Cisco IOS Software is potentially affected. Any unaffected products are listed in the companion non-IOS security advisory.

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

Details

Simple Network Management Protocol (SNMP) defines a standard mechanism for remote management and monitoring of devices in an Internet Protocol (IP) network. There are three fundamental categories of SNMP messages: "get" requests to request information, "set" requests which modify the configuration of the remote device, and "trap" messages which provide a notification or 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 results in a system crash and reload (or reboot) in most circumstances.

In most cases, the vulnerability can be mitigated by applying an access-list statement either to protect the SNMP service itself or to prevent the receipt or transport of SNMP messages at an interface. If access is only permitted for certain IP source addresses such as the IP address of a network management system, the affected device may still be vulnerable. If the network is not protected against IP source address "spoofing" with appropriate ingress filtering, an attacker may be able to transmit a packet from some other location that appears to come from the authorized network management station and successfully crash the destination device.

In some cases, access-list statements on the SNMP service do not protect the device because the vulnerability is exposed before the access-list statement is evaluated. A similar circumstance occurs in which the effectiveness of mitigation commands is negated following a reload. Due to an unrelated defect, Cisco Bug ID CSCdv48842, the effectiveness of the commands depends on the order in which they are parsed. Although effective in the running configuration, the commands are saved in the wrong order in the stored configuration. When the configuration is parsed after a reload, the commands are executed in the wrong order and the expected protection is not provided. Both of the preceding cases are documented in the Workarounds section below, including the ranges of IOS releases in which they are and are not effective.

In certain IOS releases, a community string is not actually removed until the device is reloaded. If the

community string is deleted as a protective measure, the system may still be vulnerable until the affected device is reloaded. This condition is due to an unrelated defect documented as Cisco Bug ID CSCds53023, and a workaround is provided in the section below.

In rare circumstances, an unrelated software defect with a documented workaround, Cisco Bug ID CSCdt14805, will cause an affected device to reload continuously as it attempts to recover, and will require manual intervention to resume normal operation. This behavior can be inhibited with the **logging exception 4096** command applied while in enable mode. This command does not protect against the vulnerability described in this advisory, but will allow an affected device to reload normally if it crashes due to the vulnerabilities described in this advisory.

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. The authors intend to make the test suite available to the public at the same time that this advisory is published.

The vulnerabilities are repaired by generally improving the handling of malformed SNMP messages in various ways, at a minimum by adding much stronger tests for the validity of incoming SNMP messages. 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.

Cisco Bug IDs CSCdw65903 and CSCdw62592 identify IOS software releases that have been fixed for these vulnerabilities. The following are the complete list of Bug ID's associated with this issue for IOS versions: CSCdt11503, CSCdu06427, CSCdu82770, CSCdv43903, CSCdv73848, CSCdv60119, CSCdm63334, CSCdv57565, CSCdw03959, CSCds87560, CSCin01557, CSCin01664, CSCdv48842, CSCin01208, CSCdu47447, CSCdv48776, CSCdv66527, CSCds89640, CSCdt41731, CSCdt83999, CSCea29276, CSCdw72930, CSCdx27170, CSCdw89845, CSCdx14656, CSCdv22261, CSCdw62852, CSCdt20091, CSCdv60119, CSCdw68469, CSCdt41731, CSCdv04606, CSCdw63089, CSCdu89682, CSCdw78210, CSCds89640.

There are three other notable conditions that may appear to be caused by these vulnerabilities but are actually triggered by overloaded logging mechanisms. First, a change to the logging mechanism for SNMP authentication failures introduced in 12.0(16)S can result in a flood of syslog messages. Testing for the SNMP vulnerabilities against a fixed version of IOS could result in a denial of service due to a flood of logging messages on affected systems. This behavior is repaired in 12.0(21)S by turning off the new logging behavior by default and rate-limiting the SNMP authentication failure syslog messages. A workaround is provided by applying the following undocumented command while in enable mode on the affected device: **no logging snmp-authfail**. Note that using this workaround will result in disabling all SNMP authentication failure logging messages.

Second, certain platforms are susceptible to tracebacks while testing for malformed SNMP message vulnerabilities. The tracebacks do not result in a crash, but may result in memory leaks and excessive logging which in turn may cause performance of the affected device to degrade to an unacceptable level. The performance impact can be mitigated by limiting the logging configuration to reduce the normal volume of logging messages.

Third, certain platforms and releases may encounter problems with the SNMP flash memory Management Information Base (MIB). When an "snmpwalk" of the affected device is executed, attempts to access the "flash MIB" result in a large volume of error messages which might overload the console and logging system. The performance impact can be limited as shown above.

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 10.x and earlier. It is not currently supported in nor employed by any current Cisco products. Filtering port 1993 to protect Cisco devices is only relevant in networks with Cisco devices running IOS release 8.x, 9.x., or 10.0.

Impact

The vulnerability can be exploited to produce a Denial of Service (DoS) attack. When the vulnerability is exploited, it 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. In any circumstance where ingress and egress source IP address filtering is lacking, it is more likely that an attacker could spoof the source IP address and circumvent access control mechanisms to cause a vulnerable system to fail.

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 that depends on the community string.

Software Versions and Fixes

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-non-ios-pub.shtml>.

Cisco IOS Software

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," "Interim," 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). When selecting a release, keep in mind the following definitions:

- **Maintenance** – Most heavily tested, stable, and highly recommended release of a release train in any given row of the table.
- **Rebuild** – Constructed from the previous maintenance or major release in the same train, it contains the fix for a specific defect. Although it receives less testing, it contains only the minimal changes necessary to repair the vulnerability.
- **Interim** – Built at regular intervals between maintenance releases and receives less testing. Interims should be selected only if there is no other suitable release that addresses the vulnerability. Interim images should be upgraded to the next available maintenance release as soon as possible. Interim releases are not available through manufacturing, and usually they are not available for customer download from CCO without prior arrangement with the Cisco TAC.

To find the information for a given IOS release, compare the release number as reported by the **show version** command to the major releases in the first column below. For example, if your device reports that it is running 12.0(4), find the row in the table for "12.0". Reading across to the right, you find 12.0(4b) in the Rebuild column, indicating that both 12.0(4) and 12.0(4a) are both vulnerable. Since 12.0(4b) is already available for download from CCO, you could upgrade to it immediately. The earliest maintenance release containing the fix will be 12.0(22), which will be available for download from CCO on or about 2002-Apr-08. The earliest interim release containing the fix is not available.

If a release train is labeled "Vulnerable", then migration to another release train should be considered. Except where a release label in a different release train is explicitly identified in the table below, customers should contact the Cisco TAC for assistance to identify the appropriate migration path. If migration is not possible, then workarounds may be the only alternative.

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 below.

More information on Cisco IOS software release names and abbreviations is available at <http://www.cisco.com/warp/public/620/1.html>.

The fixes will be available at the Software Center located at <http://www.cisco.com/public/sw-center/>.

For a current view of all posted and repaired images for Cisco IOS software, please check the listing available to registered CCO users at:

Train or Release	Description or Platform	Availability of First Fixed Releases*		
10.x Releases and Earlier		Rebuild	Interim**	Maintenance
10.3 and earlier	Major release for all platforms	Vulnerable		
		Not Scheduled		
11.0 Releases		Rebuild	Interim**	Maintenance
11.0	Major General Deployment release for all platforms	11.0(22b)***	Only available via FTP;	
11.0BT	Early Deployment release for 7000, 7200, 7500	2002-Feb-18 Vulnerable	see note below.	
11.0NA	ED release: 1003,1004,1005	Not Scheduled Vulnerable		
		Not Scheduled		
11.1 Releases		Rebuild	Interim**	Maintenance
11.1	Major release for all platforms	11.1(24b)***	Only available via FTP; see note below.	
		2002-Feb-27		
11.1AA	ED release for access servers: 1600, 3200, and 5200 series.	11.1(20)AA4		
11.1CA	Platform-specific support for 7500, 7200, 7000, and RSP	2002-Mar-04 11.1(36)CA3		
11.1CC	ISP train: added support for FIB, CEF, and NetFlow	2002-Feb-22 11.1(36)CC5		
		2002-Feb-25		

	on 7500, 7200, 7000, and RSP			
11.1CT	Added support for Tag Switching on 7500, 7200, 7000, and RSP	11.1(28a)CT		
11.1IA	DistributedDirector only	2002-Mar-04 11.1(28)IA2		
		2002-Mar-04		
11.2 Releases		Rebuild	Interim**	Maintenance
11.2	Major release, general deployment	11.2(26d)		
11.2BC	Platform support for IBM networking, CIP, and TN3270 on 7500, 7000, and RSP series	2002-Feb-23 Vulnerable		
11.2F	Early Deployment release for all platforms	Not Scheduled Vulnerable		
11.2GS	Early deployment release to support 12000 GSR	Not Scheduled 11.2(19)GS8		
11.2P	New platform support for all platforms	On CCO 11.2(26)P4		
11.2SA	Catalyst 2900XL switch	2002-Feb-25 11.2(8.10)SA6		
		On CCO		
11.2WA	Lightstream 1010 ATM switch	Vulnerable		
11.2XA	11.2(4)XA only: Short lived release for 1600 and 3600 only	Not Scheduled		
		11.2(4)XA2		
	11.2(9)XA only: Short lived release for 5300 only	2002-Feb-22 Vulnerable		
11.3 Releases		Rebuild	Interim**	Maintenance
11.3	Major release for all platforms	11.3(11c)		
		On CCO		
11.3AA	Early Deployment release for 5200, 5300, 5800, 7200	Vulnerable		

Not Scheduled

11.3DA	Early Deployment release for 6200 DSLAM	Vulnerable		
11.3DB	Early Deployment release for the 6400 NSP xDSL broadband concentrator	Not Scheduled 11.3(9)DB3		
11.3DC	Early Deployment release for the 6400 NRP xDSL broadband concentrator	2002-Feb-19 Vulnerable		
11.3HA	Early Deployment release for ISC3303	Not Scheduled Vulnerable		
11.3MA	Early Deployment release for MC3810	Not Scheduled 11.3(1)MA9		
11.3NA	Early Deployment release for 2500, 3600, 5300, uBR900, uBR7000	2002-Feb-19 Vulnerable		
11.3T	Early deployment major release	Not Scheduled 11.3(11b)T2		
11.3XA	11.3(2)XA only: Short lived release for uBR7000 and 2600	On CCO Vulnerable		
12.0 Releases		Not Scheduled		
12.0	General Deployment release for all platforms	Interim**	Interim**	Maintenance
		12.0(2b)		12.0(22)
		On CCO		2002-Apr-08
		12.0(3d)		
		On CCO		
		12.0(4b)		
		On CCO		
		12.0(5a)		
		On CCO		
		12.0(6b)		
		On CCO		
		12.0(7a)		
		On CCO		
12.0(8a)				

		On CCO		
		12.0(9a)		
		On CCO		
		12.0(10a)		
		On CCO		
		12.0(11a)		
		On CCO		
		12.0(12a)		
		On CCO		
		12.0(13a)		
		On CCO		
		12.0(14a)		
		On CCO		
		12.0(15a)		
		On CCO		
		12.0(16a)		
		On CCO		
		12.0(17a)		
		On CCO		
		12.0(18b)		
		2002-Feb-14		
		12.0(19a)		
		2002-Feb-12		
		12.0(20a)		
		On CCO		
		12.0(21a)		
		2002-Feb-10		
12.0DA	Early Deployment release for 6200	Vulnerable		
		Not Scheduled		
12.0DB	ISP/Telco/PTT xDSL broadband concentrator platforms	12.0(7)DB2		
12.0DC	6400 Access Concentrator	On CCO 12.0(7)DC1		
		On CCO		
		12.0(8)S1		
		On CCO		

		12.0(9)S8		
		On CCO		
		12.0(10)S7		
		On CCO		
		12.0(11)S6		
		On CCO		
		12.0(12)S3		
		On CCO		
		12.0(13)S6		
		2002-Feb-12		
		12.0(14)S7		
		On CCO		
		12.0(15)S6		
		On CCO		
		12.0(16)S8		
		On CCO		
		12.0(17)S4		
		On CCO		
		12.0(18)S5		
		On CCO		
		12.0(19)S2		
		On CCO		
		12.0(21)S1		
		On CCO		
12.0SC	Cable/broadband ISP: ubr7200	12.0(15)SC1		
		On CCO		
		12.0(16)SC3		
		On CCO		
12.0SL	Early Deployment release 10000 ESR	12.0(17)SL6		
		On CCO		
		12.0(19)SL4		
		On CCO		
12.0SP	Early Deployment release	12.0(20)SP1		
		On CCO		
		12.0(11)ST4		12.0(21)ST
		On CCO		March 2002

		12.0(14)ST3		
		On CCO		
		12.0(16)ST1		
		On CCO		
		12.0(17)ST5		
		On CCO		
		12.0(18)ST1		
		On CCO		
		12.0(19)ST2		
		On CCO		
		12.0(20)ST2		
		On CCO		
12.0SX	Other than 12.0(10)SX: Short-lived early deployment release for the 10000 ESR			12.0(21)SX
	12.0(10)SX only: Short-lived early deployment release	Vulnerable		2002-Feb-25
12.0T	Early Deployment release	Not Scheduled 12.0(7)T2		
		On CCO		
12.0W5	Early Deployment release for c5rsm images only	12.0(10)W5(18h)		
	Early Deployment maintenance release for c6msm images only	2002-Mar-07 12.0(16)W5(21c)		
	Early Deployment maintenance release for cat2948g-L3 and cat4232 images only	2002-Mar-08 12.0(18)W5(22b)		
	Early Deployment maintenance release for c5atm, cat8510c, cat8510m, cat8540c, cat8540m, and ls1010 images only	2002-Mar-04 12.0(20)W5(24a)		
		On CCO 12.0(5)WC2b		

	12.0(5)WC, 12.0(5)WC2, and 12.0(5.4)WC1 for 2900XL-LRE only	On CCO		
	12.0(5)WC2 and 12.	12.0(5)WC3b		
		On CCO		
	12.0(5)WC2, 12.0(5.3)WC1, and 12.0(5.4)WC1 for 2950 only	12.1(6)EA2b		
12.0WT	12.0(13)WT6(1) only: Short-lived early deployment release.	On CCO Vulnerable		
12.0WX	12.0(4a)WX5(11a) only: Maintenance release for c5atm, cat8510c, cat8510m, cat8540c, cat8540m, ls1010 images only	Not Scheduled 12.0(20)W5(24a)		
	12.0(7)WX5(15a) only: Maintenance release for cat2948g-L3, cat2948g-L3, and cat4232 images only	2002-Feb-12 12.0(18)W5(22b)		
12.0XA	12.0(1)XA only: Short-lived early deployment release	2002-Feb-22 Vulnerable		
12.0XB	12.0(1)XB only: Short-lived early deployment release	Not Scheduled Vulnerable		
12.0XC	12.0(2)XC only: Short-lived early deployment release	Not Scheduled Vulnerable		
12.0XD	12.0(2)XD only: Short-lived early deployment release	Not Scheduled Vulnerable		
	12.0(1)XE only: Short-lived early deployment release	Not Scheduled Vulnerable		
	12.0(2)XE only: Short-lived early deployment release	Not Scheduled 12.0(2)XE4		
		On CCO		

12.0XE

	12.0(3)XE only: Short-lived early deployment release	Vulnerable		
	12.0(4)XE only: Short-lived early deployment release	Not Scheduled 12.0(4)XE2		
	12.0(5)XE only: Short-lived early deployment release	On CCO 12.0(5)XE8		
	12.0(7)XE only: Short-lived early deployment release	On CCO 12.0(7)XE2		
12.0XF	12.0(7)XF only: Short-lived early deployment release	On CCO Not Affected		
	12.0(2)XF only: Short-lived early deployment release	Not Affected		
12.0XG	12.0(3)XG only: Short-lived early deployment release	Vulnerable		
12.0XH	12.0(2)XH only: Short-lived early deployment release	Not Scheduled Vulnerable		
	12.0(4)XH only: Short-lived early deployment release	Not Scheduled Vulnerable		
12.0XI	12.0(4)XI only: Short-lived early deployment release	Not Scheduled Vulnerable		
12.0XJ	12.0(4)XJ only: Short-lived early deployment release	Not Scheduled Vulnerable		
12.0XK	12.0(5)XK only: Short-lived early deployment release	Not Scheduled 12.0(5)XK2		
	12.0(7)XK only: Short-lived early deployment release	On CCO 12.0(7)XK3		
12.0XL	12.0(4)XL only: Short-lived early deployment release	On CCO Vulnerable		
12.0XM	12.0(4)XM only: Short-lived early deployment release	Not Scheduled 12.0(4)XM1		
12.0XN	12.0(5)XN only:	On CCO 12.0(5)XN1		

	Short-lived early deployment release	2002-Feb-22		
12.0XP	12.0(5)XP and 12.0(5.1)XP only: Early Deployment release for 2900XL and 3500XL only	12.0(5)WC3b		
12.0XT	12.0(5)XT only: Short-lived early deployment release	On CCO Vulnerable		
12.0XU	12.0(5)XU and 12.0(5.2)XU only: Early Deployment release for 2900XL and 3500XL only	Not Scheduled 12.0(5)WC3b		
12.0XV	12.0(7)XV only: Short-lived early deployment release	On CCO Vulnerable		
12.1 Releases		Not Scheduled		
		Interim**	Interim**	Maintenance
12.1	Major Release, all platforms	12.1(1c)		12.1(13)
		On CCO		2002-Feb-14
		12.1(2b)		
		On CCO		
		12.1(3b)		
		On CCO		
		12.1(4a)		
		On CCO		
		12.1(5e)		
		On CCO		
		12.1(6a)		
		On CCO		
		12.1(7b)		
		On CCO		
		12.1(8c)		
		On CCO		
		12.1(9a)		
		On CCO		
		12.1(10a)		
On CCO				
12.1(11b)				

		On CCO		
		12.1(12b)		
		On CCO		
12.1AA	Early deployment release Dial support	12.1(8)AA1		
12.1CX	12.1(4)CX only: Short-lived early deployment release	On CCO Vulnerable		
	12.1(7)CX1 only: Short-lived early deployment release	Not Scheduled Vulnerable		
12.1DA	Early Deployment release, xDSL support for 6100 and 6200	Not Scheduled 12.1(7)DA3		
12.1DB	Early Deployment release for the 6400 NSP	2002-Mar-04 12.1(1)DB2		
		On CCO		
		12.1(3)DB1		
		2002-Mar-04		
		12.1(4)DB2		
		On CCO		
		12.1(5)DB1		
12.1DC	Early Deployment release for the 6400 NRP	On CCO		
		12.1(1)DC2		
		On CCO		
		12.1(3)DC2		
		On CCO		
		12.1(4)DC3		
		On CCO		
	Early Deployment release, Core/ISP support for 7100, 7200, RSP, 7500 platforms	12.1(1)E5		
	Early Deployment release, Core/ISP support for c6msfc and c6sup images only	On CCO 12.1(1)E6		
		On CCO		

	Early Deployment release, Core/ISP support for rsp, c7000, cat5k, and cat6k images only	12.1(2)E2		
		On CCO		
		12.1(3a)E7		
		On CCO		
		12.1(4)E3		
		On CCO		
		12.1(5c)E12		
		On CCO		
		12.1(6)E8		
		On CCO		
		12.1(7a)E5		
		2002-Feb-25		
		12.1(7a)E6		
		On CCO		
		12.1(8b)E9		
		On CCO		
		12.1(9)E3		
		On CCO		
		12.1(10)E4		
		On CCO		
	Early Deployment release, Core/ISP support for 7100, RSP, and 7500 platforms, and c5msfc, c6msfc2, c6sup11, and c6sup12 images only	12.1(3a)E7		
		On CCO		
	Early Deployment release, Core/ISP support for the 7200 platform	12.1(3a)E8		
		On CCO		
12.1EA	12.1(6)EA2 for 2950 only	12.1(3a)E8		
		On CCO		
	12.1(4)EA1e for 3550 only	12.1(6)EA2b		
		On CCO		
12.1(6)EA1 for 3550 only	12.1(8)EA1c			
	On CCO			
12.1EC		12.1(8)EC1		

	Early Deployment release, Core/ISP support for the uBR7200 only	On CCO		
		12.1(9)EC1		
		On CCO		
		12.1(10)EC1		
		On CCO		
12.1EW	12.1(8a)EW only: Short-lived early deployment release	12.1(8a)EW1		
12.1EX	12.1(1)EX only: Short-lived early deployment release	2002-Mar-04 12.1(1)EX1		
	12.1(5)EX only: Short-lived early deployment release	2002-Mar-04 12.1(5c)EX3		
	12.1(6)EX only: Short-lived early deployment release	2002-Mar-04 Vulnerable		
	12.1(8a)EX only: Short-lived early deployment release	Not Scheduled 12.1(8b)EX4		
	12.1(9)EX only: Short-lived early deployment release	On CCO 12.1(9)EX3		
	12.1(10)EX only: Short-lived early deployment release	On CCO		12.1(10)EX
12.1EY	12.1(5)EY only: Short-lived early deployment release	12.1(5)EY2		On CCO
	12.1(6)EY only: Short-lived early deployment release	On CCO 12.1(6)EY1		
	12.1(7a)EY only: Short-lived early deployment release	On CCO 12.1(7a)EY3		
12.1T	Early deployment release all major platforms	On CCO 12.1(5)T12		
12.1XA	12.1(1)XA only: Short-lived early deployment release	On CCO Vulnerable		
12.1XB	12.1(1)XB only: Short-lived early deployment release	Not Scheduled Vulnerable		
12.1XC		Not Scheduled 12.1(1)XC1		

	12.1(1)XC only: Short-lived early deployment release	On CCO		
12.1XD	12.1(1)XD only: Short-lived early deployment release	Vulnerable		
12.1XE	12.1(1)XE only: Short-lived early deployment release	Not Scheduled 12.1(1)XE1		
12.1XF	12.1(2)XF only: Short-lived early deployment release	2002-Feb-22 12.1(2)XF5		
12.1XG	12.1(3)XG only: Short-lived early deployment release	On CCO 12.1(3)XG6		
12.1XH	12.1(2a)XH only: Short-lived early deployment release	On CCO Vulnerable		
12.1XI	12.1(3)XI only: Short-lived early deployment release	Not Scheduled 12.1(3a)XI8		
12.1XJ	12.1(3)XJ only: Short-lived early deployment release	On CCO Vulnerable		
12.1XL	12.1(3)XL only: Short-lived early deployment release	Not Scheduled Vulnerable		
12.1XM	12.1(5)XM only: Short-lived early deployment release	Not Scheduled 12.1(5)XM7		
12.1XP	12.1(3)XP only: Short-lived early deployment release	On CCO Vulnerable		
12.1XQ	12.1(3)XQ only: Short-lived early deployment release	Not Scheduled Vulnerable		
12.1XR	12.1(5)XR only: Short-lived early deployment release	Not Scheduled 12.1(5)XR2		
12.1XS	12.1(3)XS only: Short-lived early deployment release	2002-Mar-04 Vulnerable		
12.1XS	12.1(5)XS only: Short-lived early deployment release	Not Scheduled Vulnerable		
12.1XT	12.1(3)XT only:	Not Scheduled Vulnerable		

	Short-lived early deployment release	Not Scheduled		
12.1XU	12.1(5)XU only: Short-lived early deployment release	Vulnerable		
12.1XV	12.1(5)XV only: Short-lived early deployment release	Not Scheduled 12.1(5)XV4		
12.1XW	12.1(3)XW only: Short-lived early deployment release	On CCO Vulnerable		
12.1XX	12.1(5)XX only: Short-lived early deployment release	Not Scheduled Vulnerable		
12.1YA	12.1(5)YA only: Short-lived early deployment release	Not Scheduled 12.1(5)YA2		
12.1YB	12.1(5)YB only: Short-lived early deployment release	On CCO 12.1(5)YB5		
12.1YC	12.1(5)YC only: Short-lived early deployment release	On CCO 12.1(5)YC2		
12.1YD	12.1(5)YD only: Short-lived early deployment release	On CCO 12.1(5)YD6		
12.1YE	12.1(5)YE only: Short-lived early deployment release	On CCO Vulnerable		
12.1YF	12.1(5)YF only: Short-lived early deployment release	Not Scheduled 12.1(5)YF4		
12.1YH	12.1(5)YH only: Short-lived early deployment release	2002-Mar-04 12.1(5)YH3		
12.1YI	12.1(5)YI only: Short-lived early deployment release	On CCO 12.1(5)YI2		
12.2 Releases		2002-Mar-04 Rebuild	Interim**	Maintenance
12.2	Major release for all platforms	12.2(1d)		
		On CCO		
		12.2(3d)		
		On CCO		
		12.2(5d)		

		On CCO		
		12.2(6c)		
		On CCO		
		12.2(7a)		
		2002-Mar-04		
12.2B	Early Deployment Broadband Release	12.2(2)B4		
		2002-Mar-04		
		12.2(4)B2		
		On CCO		
12.2BC	Early Deployment Broadband Release for the uBR7000 and uBR10000	12.2(4)BC1a		
12.2BY	Short-lived early deployment release	On CCO 12.2(2)BY2		
		2002-Mar-04		
		12.2(2)BY3		
		2002-Feb-22		
12.2DA	Early Deployment release, xDSL support for the 6100 and 6200	12.2(1b)DA1		12.2(7)DA
		On CCO		On CCO
		12.2(5)DA1		
		2002-Mar-04		
12.2DD	Specific Technology Early Deployment release for 7200 and 7400	12.2(2)DD3		
12.2DX	12.2(1)DX only: Short-lived early deployment release	On CCO 12.2(1)DX1		
12.2MB	Specific Technology Early Deployment release for 2600 and 7500	On CCO 12.2(4)MB3		
12.2MX	12.2(4)MX only: Short-lived early deployment release	On CCO 12.2(4)MX1		
12.2T	Early deployment release for all major platforms	2002-Feb-22 12.2(2)T4		12.2(8)T
		On CCO		2002-Feb-25
		12.2(4)T3		
		On CCO		

12.2XA	12.2(1)XA only: Short-lived early deployment release	12.2(2)XA5		
12.2XB	12.2(2)XB only: Short-lived early deployment release	On CCO 12.2(2)XB3		
12.2XC	12.2(1a)XC only: Short-lived early deployment release	On CCO Vulnerable		
	12.2(2)XC only: Short-lived early deployment release	Not Scheduled Vulnerable		
12.2XD	12.2(1)XD only: Short-lived early deployment release	Not Scheduled 12.2(1)XD3		
12.2XE	12.2(1)XE only: Short-lived	On CCO 12.2(1)XE2		
		On CCO		
12.2XF	12.2(1)XF1 only: Short-lived early deployment release	Vulnerable		
	12.2(2)XF only: Short-lived early deployment release	Not Scheduled Vulnerable		
	12.2(4)XF only: Short-lived early deployment release	Not Scheduled Vulnerable		
12.2XG	12.2(2)XG only: Short-lived early deployment release	Not Scheduled 12.2(2)XG1		
12.2XH	12.2(2)XH only: Short-lived early deployment release	2002-Feb-22 12.2(2)XH2		
12.2XI	12.2(2)XI only: Short-lived early deployment release	On CCO 12.2(2)XI1		
12.2XJ	12.2(2)XJ only: Short-lived early deployment release	On CCO 12.2(2)XJ1		
12.2XK	12.2(2)XK only: Short-lived early deployment release	2002-Mar-04 12.2(2)XK2		
12.2XL	12.2(4)XL only: Short-lived early deployment release	On CCO 12.2(4)XL3		
12.2XM	12.2(4)XM only: Short-lived early	On CCO 12.2(4)XM2		

	deployment release	On CCO		
12.2XN	12.2(2)XN only: Short-lived early deployment release	12.2(2)XN		
12.2XQ	12.2(2)XQ only: Short-lived early deployment release	2002-Feb-22 12.2(2)XQ2		
12.2XS	12.2(1)XS only: Short-lived	2002-Mar-04 12.2(1)XS2		
		On CCO		
12.2XT	12.2(2)XT only: Short-lived early deployment release	12.2(2)XT2		
12.2XU	12.2(2)XU only: Short-lived early deployment release	2002-Mar-04 12.2(2)XU2		
12.2XW	12.2(4)XW only: Short-lived early deployment release	2002-Mar-01 12.2(4)XW1		
12.2YA	12.2(4)YA only: Short-lived early deployment release	2002-Mar-04 12.2(4)YA1		

2002-Mar-04

NOTES:

* All dates are tentative and subject to change.

** Interim releases receive the less testing than Maintenance or Rebuild releases. Interim release labels are provided to identify vulnerable pre-existing Interim releases. A first fixed Interim release should be used only when no other suitable release is available.

*** 11.0(22b) and 11.1(24b) can only be obtained via File Transfer Protocol (FTP) to the host ftp.cisco.com using your CCO username and password. If using a command-line ftp client, use the following commands to retrieve 11.0(22b) :

```
ftp ftp.cisco.com
Name: your-CCO-username
Password: your-CCO-password
cd /cisco/ios/11.0/11.0.22b
ls
```

Identify your platform, for example, "2500" for the 2500 series router, and then change into that directory:

```
cd your-router-platform
ls
```

Identify the filename for the desired binary image, and then set binary mode and turn on hash-mark printing before downloading it:

```
bin
hash
get binary-image-filename
quit
```

If you are using a browser to download the files via FTP, you will need to specify your CCO username and CCO password as part of the URL, for example:

```
ftp://your-CCO-username:your-CCO-password@ftp.cisco.com
```

Once you have connected, the URL will change to:

```
ftp://your-CCO-username@ftp.cisco.com
```

Then browse to the "cisco" directory, the "ios" directory, and the "11.0" and "11.0.22b" directories as shown above to find your platform and desired binary image file. Then click on the filename to download it.

To retrieve 11.1(24b) images, follow the previous instructions, substituting 11.1.24b in place of 11.0.22b.

If you do not have a valid CCO account, then you should request the fixed software via the Cisco TAC as shown below.

Workarounds

The usefulness of any workaround is dependent on specific customer situations such as products, software versions, network topology, traffic behavior, and organizational mission. Due to the great variety of affected products and releases, customers should carefully evaluate each workaround to ensure it is appropriate for use in the intended network before it is deployed.

Workarounds for IOS devices and Catalyst switches that run Cisco IOS software are shown below.

Workarounds for CatOS and other non-IOS products are provided in

<http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-non-ios-pub.shtml#noniosworkarounds>, the companion to this security advisory.

General Measures

- Turn SNMP off in the device. This is an effective workaround, but removes management capability to the device. This can be done using the following **configure** command:

```
no snmp-server
```

Removing the community string public with the **configure** command: **no snmp-server community public 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. Verify SNMP server status by using the enable command **show snmp**. You should see a response of "%SNMP agent not enabled".

- Apply an extended access list (ACL) to deny protocol UDP, port 161 and 162, at the interface level such that SNMP access to the device is allowed only from the network management workstations. This can be done using the following **configure** commands:

```
access-list 100 permit ip host 1.1.1.1 any
access-list 100 deny udp any any eq snmp
access-list 100 deny udp any any eq snmptrap
access-list 100 permit ip any any
```

where 1.1.1.1 is the trusted network management station. This access list must be applied to all interfaces using the following **configure** commands:

```
interface serial 0 ip
access-group 100 in
```

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.

The access-list statement containing "snmptrap" will prevent notification messages from entering the

network when it is applied at the network edge.

Note: For the preceding workaround to be effective on a Layer 2 Catalyst switch (2900XL, 3500XL, 2950) running Cisco IOS software, the access-list must be applied to the management VLAN interface. The preceding workaround is NOT EFFECTIVE for Catalyst 8500s without ACL daughter cards, Catalyst 2948G-L3 10/100 ports, Catalyst 6000 MSM, and LightStream 1010 ATM Switches.

The Cisco SAFE white papers cover techniques that can be used to control IP address spoofing. These papers can be found at:

[Cisco SAFE Solution](#)

Two white papers cover securing your network in general and controlling IP address spoofing specifically:

[SAFE: A Security Blueprint for Enterprise Networks](#)

[SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks](#)

Do not use a community string of "public" for any reason. Many attacks assume a "public" community string is available on the target device, and removing it may reduce the risk of a successful attack. Since a community string is transported in clear text, and tools and test suites can easily be modified to use other community strings, it is important to use a community access-list (ACL) to further reduce the risk.

Workarounds with Caveats

The workarounds with caveats in the following section are effective in the following Cisco IOS software releases:

- 11.0, 11.1, 11.2 and derivatives in 11.x
- 12.0(3)T and later 12.0T
- 12.0(6)S and later 12.0S
- 12.0(8.6)ST through 12.0(19.1)ST, 12.0(19.6)ST and later
- 12.1
- 12.1(1)T up to 12.1(4.4)T
- 12.1(1)E up to 12.1(9.4)E
- 12.1(1)EC up to 12.1(9.4)EC
- 12.1EY

The workarounds with caveats are NOT EFFECTIVE in (and should not be applied to) the following Cisco IOS software releases:

- 11.3, 11.3T
- 12.0
- 12.0(1)S through 12.0(5.x)S
- 12.0(19.3)ST, 12.0(19.3)ST1, 12.0(19.3)ST2
- 12.0W5
- 12.1(4.4)T2 and later 12.1T
- 12.1(9.5)E and later 12.1E
- 12.1(9.5)EC and later 12.1EC
- 12.2, 12.2T

Best current practices recommend applying ACLs to community strings and ensuring that the community strings for requests are not identical to community strings used for notifications. Access-lists provide further protection when used in combination with other protective measures. Using different community strings for requests and trap messages reduce the likelihood of further attacks or compromises if the community string is discovered by an attacker, whether by compromising a remote device or by sniffing a trap message from the network without authorization.

Apply an SNMP community-based ACL to allow SNMP access to the device **only** from the network management workstations using the following **configure** commands:

access-list 1 permit 1.1.1.1

snmp-server community string1 ro 1

In this example the trusted management station is configured with an IP address of 1.1.1.1. Apply an access list to all of the read-only and read-write community strings configured on the device.

If community strings are also configured for notifications, they must be different than the community strings used for requests in order for this workaround to be effective. This is considered a best current practice with SNMP configuration, and it also avoids unrelated issues with some Cisco IOS software releases. The SNMP community strings for read-only or read-write access should be protected against unauthorized disclosure from receiving or sniffing a notification message.

Use the following **configure** commands to change community strings for notifications that are the same as community strings used for requests.

no snmp-server host 1.1.1.1 string1

snmp-server community string1 ro 1

The second command above reapplies the access list to the community and must be re-entered after the **snmp-server host** command is entered to ensure the access list is applied correctly in some Cisco IOS software releases.

Use the following **configure** command to tell the device to send notifications using the new community string:

```
snmp-server host 1.1.1.1 anythingbutstring1
```

All community strings used for notifications, like the "anythingbutstring1" community string above, need to be set to deny all SNMP requests. Use the following **configure** commands to do this:

access-list 2 deny any

snmp-server community anythingbutstring1 ro 2

This is required because Cisco IOS software configures community strings used for notifications with no read or write view. You cannot see or change any information on the device using this string.

However, requests using a community string with no view will still be processed by the device and an SNMP tool could exploit this processing and crash the device.

Please note that in order for this to take effect, the commands must be issued in the following order:

snmp-server host 1.1.1.1 anythingbutstring1

snmp-server community anythingbutstring1 ro 2

This configuration will not survive a reload.

In certain releases, entering the **snmp-server community** command will delete the notify view required to send traps. This can be determined by running this command while in enable mode:

show snmp group

Look for two or more groups with the same name as the community string used for notifications. The output should look like this:

```
groupname: anythingbutstring1          security model:v1
readview :vldefault                    writeview:<no writeview specified>
notifyview: *tv.FFFFFFFF.FFFFFFFF
row status: active          access-list: 2

groupname: anythingbutstring1          security model:v2c
readview :vldefault                    writeview:<no writeview specified>
notifyview: <no notifyview specified>
row status: active          access-list: 2
```

Ensure that the notifyview is set for the version of notifications you want the device to send, and that the access-list is set correctly for all security models.

If either fields are not correct, first reapply the **configure** command:

snmp-server host 1.1.1.1 anythingbutstring1

Then look at the output of **show snmp group** again. Take the view listed as the notifyview, the

- correct access–list number, and the security model version and enter the following **configure** command:
snmp–server group anythingbutstring1 v1 notify *tv.FFFFFFFF.FFFFFFFF access 2
 Modify the above command to match your configuration. Verify this worked using the **show snmp group** enable command. If you are sending notifications using this community string with both SNMPv1 and SNMPv2c, then you'll need to enter this command twice – the first time specifying the version as "v1", and the second time as "v2c".

Note: The **snmp–server group** command will show up in the configuration before the **snmp–server host** command, so this part of the workaround will not survive a reboot. After a reboot, the device will continue to send traps but the **snmp–server group** command will need to be re–entered to protect the device from exploits using this community string.

- Change the community string from "public" to something not so obvious. Attackers typically assume "public" can be used to gain access to SNMP services.

Note: Even though the current version of the PROTOS tests will not crash the Cisco IOS device if the device community string is not set to "public", it is very easy to modify the PROTOS code so that other community string values are used. Therefore, it is important to use a community ACL as described above to further mitigate the risk.

Workaround for CSCds53023

The following workaround should be applied if an SNMP community has been removed using the **no snmp–server community** command, but still appears to be configured on the device and it is not feasible to reload the device.

Since IOS represents all community strings as SNMPv3 groups, you can delete community strings using the **no snmp–server group** configuration command instead.

Enter the enable command **show snmp group**. Any groups that show up that should not be there should be deleted. Note that the "ILMI" group is required to allow ATM ILMI to operate and should not be deleted. The ILMI community string does not present a security issue as it is tied to the ILMI transport protocol.

Use the configuration command **no snmp–server group** to delete groups. For example, if you have deleted a community string using the following command:

```
no snmp–server community public
```

But when you execute the **show snmp group** command you see:

```
groupname: public                security model:v1
readview :<no readview specified> writeview:<no writeview specified>
notifyview:<no notifyview specified>
row status: active

groupname: public                security model:v2c
readview :<no readview specified> writeview:<no writeview specified>
notifyview:<no notifyview specified>
row status: active
```

Note: If the notify view is filled in be sure to check and verify if this community string is still being used for notifications. If it is in use, then do not delete these groups. Doing so will stop the router from sending notifications using this community string.

To delete this community string, delete both groups using the following configuration command:

```
no snmp-server group public v1 no snmp-server group public v2c
```

Then run the enable command **show snmp group** again to ensure that the groups have been removed.

Troubleshooting Tips for Cisco IOS Software

- Configure the startup-config with no SNMP and the running-config with the SNMP. In the event of a successful exploit due to this vulnerability, the affected device will reload with a new configuration in which SNMP is disabled. This will prevent additional, repeated exploit of the vulnerability.
- Configure the SNMP Community ACLs with the "log" keyword. Monitor syslog for failed attempts.
- Periodically check SNMP for errors.

Configuration Notes

- **show snmp**

Command output:

```
router#show snmp
Chassis: 21350479
17005 SNMP packets input
  37 Bad SNMP version errors **
 15420 Unknown community name **
  0 Illegal operation for community name supplied
 1548 Encoding errors **
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
 0 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs
```

Watch the counters marked ** for unexpected increases in error rates that may indicate attempted exploitation of these vulnerabilities.

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-20020212-snmpp-msgs.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 2.2	2003-Dec-23	Advisory changed from INTERIM to FINAL status – updated Details section with complete list of Bug ID's associated with this advisory
Revision 2.1	2002-Mar-14	Modifications made to the Software Versions and Fixes section
Revision 2.0	2002-Feb-28	Modifications made to the following sections: Products Affected, Products Not Affected, and Software Versions and Fixes
Revision 1.5	2002-Feb-20	Modifications made to the following sections: Products Affected, Products Not Affected, Software Versions and Fixes, and Workarounds with Caveats
Revision 1.4	2002-Feb-16	Modifications made to the following sections: Summary, Details, Lists of Products Affected and Products Not Affected, table for Cisco IOS fixed images, Workarounds, Workarounds with Caveats, Troubleshooting Tips
Revision 1.3	2002-Feb-14	Added Table of Contents; updated table for Cisco IOS fixed images; "Workarounds" section updated
Revision 1.2	2002-Feb-13	Lists of Products Affected and Products Not Affected updated

Revision 1.1	2002-Feb-13	Lists of Products Affected and Products Not Affected updated; Details section updated; correction to "Applying extended access list"
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 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>.

[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: Dec 23, 2003

Document ID: 19294
