

Cisco Security Advisory: Vulnerabilities in SNMP Message Processing

Advisory ID: cisco-sa-20040420-snmp

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml>

Revision 1.5

Last Updated 2004 May 05 2330 UTC (GMT)

For Public Release 2004 April 20 2100 UTC (GMT)

Please provide your **feedback** on this document.

Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Impact](#)
- [Software Versions and Fixes](#)
- [Workarounds](#)
- [Obtaining Fixed Software](#)
- [Exploitation and Public Announcements](#)
- [Status of This Notice: INTERIM](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

Summary

Cisco Internetwork Operating System (IOS) Software release trains 12.0S, 12.1E, 12.2, 12.2S, 12.3, 12.3B and 12.3T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload.

The vulnerability is only present in certain IOS releases on Cisco routers and switches. This behavior

was introduced via a code change and is resolved with CSCed68575.

This vulnerability can be remotely triggered. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS).

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml>.

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

☐ **Affected Products**

This section provides details on affected products.

☐ **Vulnerable Products**

This vulnerability was introduced by a code change for CSCeb22276. This change was committed to the following releases, causing these releases to be vulnerable.

Cisco Catalyst ATM modules running Cisco IOS software are not affected.

The ONS 15454 and 15454E, when configured with an ML-series line card and running release 4.60 are vulnerable. The ONS 15454 and 15454E software bundles a vulnerable version of Cisco IOS software that runs on the ML-series line card. Configurations without an ML-series line card running the affected releases are not vulnerable. Release 4.60 bundles 12.1(20)EO, which is vulnerable.

The following CCO posted releases are known to be vulnerable to the SNMP issue. To Cisco's best knowledge, no other posted releases are affected. Cisco may modify this list, however, in the event of any updates. Interim or custom releases that were published by Cisco may also be vulnerable. For more information on Interim builds, see section 3.6 of <http://www.cisco.com/warp/public/620/1.html>.

Please see the [Software Versions and Fixes](#) section of this advisory for the complete Cisco IOS software upgrade table.

- 12.0(23)S4
- 12.0(23)S5
- 12.0(24)S4
- 12.0(24)S4a
- 12.0(24)S5
- 12.0(26)S1
- 12.0(27)S
- 12.0(27)SV
- 12.0(27)SV1
- 12.1(20)E
- 12.1(20)E1
- 12.1(20)E2
- 12.1(20)EA1
- 12.1(20)EB

- 12.1(20)EC
- 12.1(20)EC1
- 12.1(20)EO
- 12.1(20)EU
- 12.1(20)EW
- 12.1(20)EW1
- 12.2(12g)
- 12.2(12h)M1
- 12.2(12h)
- 12.2(20)S
- 12.2(20)S1
- 12.2(20)SW
- 12.2(21)
- 12.2(21a)
- 12.2(21)SW
- 12.2(21)ZQ
- 12.2(23)
- 12.3(2)XC1
- 12.3(2)XC2
- 12.3(2)XE
- 12.3(2)XF
- 12.3(4)T
- 12.3(4)T1
- 12.3(4)T2
- 12.3(4)T2a
- 12.3(4)T3
- 12.3(4)XD
- 12.3(4)XD1
- 12.3(4)XG
- 12.3(5)
- 12.3(5a)B
- 12.3(5a)
- 12.3(5b)
- 12.3(6)

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

☐ Products Confirmed Not Vulnerable

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

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

☐ Details

The Simple Network Management Protocol (SNMP) defines a standard mechanism for remote management and monitoring of devices in an Internet Protocol (IP) network. A device or host that supports SNMP is an SNMP entity. There are two classes of SNMP entities: SNMP managers that request information and receive unsolicited messages and SNMP agents that respond to requests and send unsolicited messages. SNMP entities that support SNMP proxy functions combine the functions of both SNMP manager and SNMP agent.

There are two classes of SNMP operations: solicited operations such as 'get' or 'set', with which the SNMP manager requests or changes the value of a managed object on an SNMP agent; and unsolicited operations such as 'trap' or 'inform' messages with which the SNMP agent provides an unsolicited notification or alarm message to the SNMP manager. The 'inform' operation is essentially an acknowledged 'trap'.

All SNMP operations are transported over the User Datagram Protocol (UDP). Solicited operations are sent by the SNMP manager to the UDP destination port 161 on the agent. Unsolicited operations are sent by the SNMP agent to the UDP destination port 162. In IOS, The acknowledgement sent by the SNMP manager to an SNMP agent in reply to an 'inform' operation is sent to a randomly chosen high port that is chosen when the SNMP process is started.

As IOS implements both an SNMP agent and SNMP proxy functionality, the SNMP process in IOS starts listening for SNMP operations on UDP ports 161, 162 and the random UDP port at the time it is initialized. The SNMP process is started either at the time the device boots, or when SNMP is configured.

The high port is chosen via the following series of steps:

1. A random number between 49152 and 59152 is generated.
2. IOS checks to see if that UDP port is already being used. If not, that UDP port is selected to receive SNMP 'inform' acknowledge messages.
3. If the port is already in use, IOS increments the port number by 1, and checks again, incrementing until an open port is found.

Therefore, the port chosen may be higher than 59152 although this is considered unlikely.

In this vulnerability, the IOS SNMP process is incorrectly attempting to process SNMP solicited operations on UDP port 162 and the random UDP port. Upon attempting to process a solicited SNMP operation on one of those ports, the device can experience memory corruption and may reload.

SNMPv1 and SNMPv2c solicited operations to the vulnerable ports will perform an authentication check against the SNMP community string, which may be used to mitigate attacks. Through best practices of hard to guess community strings and community string ACLs, this vulnerability may be mitigated for both SNMPv1 and SNMPv2c. However, any SNMPv3 solicited operation to the vulnerable ports will reset the device. If configured for SNMP, all affected versions will process SNMP version 1, 2c and 3 operations.

This vulnerability was introduced by DDTS CSCeb22276 and has been corrected with DDTS CSCed68575.

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

☐ Impact

Successful exploitation of this vulnerability results in a reload of the device. Repeated exploitation could result in a sustained DoS attack.

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

☐ Software Versions and Fixes

Be advised that Cisco released multiple advisories on 2004-April-20.

When considering software upgrades, please also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

Each row of the Cisco IOS software table (below) describes a release train. 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 12.3(5), find the row in the table for "12.3". Reading across to the right, you find 12.3(5c) in the Rebuild column, indicating that 12.3(5) through 12.3(5b) are vulnerable. Since 12.3(5c) is already available for download from CCO, you could upgrade to it as soon as possible.

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/>.

Major Release	Availability of Repaired Releases		
Affected 12.0 - Based Release	Rebuild	Interim	Maintenance
12.0S	12.0(23)S6		
	12.0(24)S6		
	12.0(26)S2		
	12.0(27)S1		
12.0SV	12.0(27)SV2 - contact TAC. Available upon request.		
Affected 12.1 - Based Release	Rebuild	Interim	Maintenance
12.1E	12.1(20)E3		
	12.1(22)E1		

12.1EA	12.1(20) EA1a		
12.1EB			12.1(22)EB
12.1EC	12.1(20)EC2 - contact TAC. Available upon request.		
12.1EO	12.1(20)EO1		
12.1EU	12.1(20)EU1 due on CCO early May, 2004		
12.1EW	12.1(20)EW2		
Affected 12.2 - Based Release	Rebuild	Interim	Maintenance
12.2	12.2(12i)		
	12.2(21b)		
		12.2(23.6) - available upon request.	12.2(24)
	12.2(23a)		
12.2S	12.2(20)S2		
			12.2(22)S
12.2SW			12.2(23)SW - available mid- May 2004
Affected 12.3 - Based Release	Rebuild	Interim	Maintenance
12.3	12.3(5c)		
	12.3(6a)		
		12.3(7.7) - available upon request.	12.3(9) - due on CCO mid-June 2004.
	12.3(5)B1 -		

12.3B	due on CCO mid-June 2004.		
12.3T	12.3(4)T4		
			12.3(7)T
12.3XC	Vulnerable, migrate to 12.3(8)T due on CCO mid-May 2004		
12.3XD	12.3(4)XD2		
12.3XE	Vulnerable, migrate to 12.3(8) T due on CCO mid-May 2004		
12.3XF	Contact TAC		
12.3XG	12.3(4)XG1		
12.3XH			12.3(4)XH
12.3XK			12.3(4)XK
12.3XQ			12.3(4)XQ

Optical Products	
Product	Availability of Repaired Release
Cisco ONS 15454 and 15454E with an ML-series Line	4.62, Available 2004- Apr-27

[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.

- It is possible to disable SNMP processing on the device running IOS by issuing the following command:

```
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. Verify SNMP server status by using the enable command **show snmp**. You should see a response of "% SNMP agent not enabled".

- Access Control Lists (ACLs) can be used to deny traffic to the affected ports. As there can be no guarantee that the random high port will fall in the range of 49152 to 59152 (possibly as high as 65535), the example access-lists below show how to block all UDP ports in the range 49152 to 65535. Care should be taken to understand the potential side effects noted later in this section.

Although Cisco IOS devices have community-string access lists which check the source address of SNMP requests per community string, they will not be sufficient to mitigate this vulnerability due to the SNMPv3 exploitation vector.

On platforms that do not have the option to use rACLs, 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 range 161 162
access-list 101 permit udp host 10.1.1.1 host 192.168.10.1 range 49152 65535
access-list 101 deny udp any host 192.168.10.1 range 161 162
access-list 101 deny udp any host 192.168.10.1 range 49152 65535
access-list 101 deny udp any host 172.16.1.1 range 161 162
access-list 101 deny udp any host 172.16.1.1 range 49152 65535
access-list 101 permit ip any any
```

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

```
interface ethernet 0/0
ip access-group 101 in
```

Note that UDP traffic in the ranges specified above must be explicitly blocked to each IP address on the router to prevent the router from accepting and processing the SNMP packets. Additionally, while blocking traffic to port 161 from unknown hosts is a best practice, in this case, port 161 is not affected and need not be blocked to prevent exploitation.

All devices that communicate directly with the router on those UDP ports will need to be specifically listed in the above access list. Cisco IOS uses ports in the range 49152 to 65535 as the source port for outbound sessions such as DNS queries.

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.

IMPORTANT NOTE: Cisco IOS uses the same source port range when upgrading via TFTP. If your upgrade process includes downloading from a TFTP server, be sure to permit UDP traffic in the range 49152 to 65535 between the router and the TFTP server. Alternative download methods that do not rely on UDP, such as FTP, may also be used.

Besides TFTP, other potentially affected services include Network Time Protocol (NTP), Remote Authentication Dial In User Service (RADIUS) and Domain Name Service (DNS). To

minimize the impact of this workaround, you may want to explicitly permit access between your IOS device and the servers providing the service(s). It is critically important that you understand the impact to your network before deploying the above workaround.

- **Blocking Individual Ports**

The high port number chosen by the IOS device can be determined by using the command **show ip sockets**. UDP traffic to that individual port can be blocked, rather than the entire port range. This approach is not ideal because the high port is chosen at random when the router is rebooted or the SNMP service is stopped and restarted. This may, however, be a short term solution for customers that want to protect themselves from the vulnerability as they prepare to upgrade, for example.

Output of the **show ip sockets** command:

```
Router#sh ip sockets
Proto      Remote      Port      Local      Port      In Out Stat TTY Output
[snip]
17  --listen--      192.168.10.72      161      0  0  1  0
17  --listen--      192.168.10.72      162      0  0  11 0
17  --listen--      192.168.10.72      49212     0  0  11 0
```

The above example shows that there are 3 SNMP-related ports listening, and the high port is bound to 49212.

Rather than blocking the entire port range from 49152 to 65535, port 49212 can be blocked (in addition to port 162) as a temporary workaround.

- **Receive ACLs (rACL)**

For distributed platforms, rACLs may be an option starting in Cisco IOS Software Versions 12.0(21)S2 for the 12000 series GSR and 12.0(24)S for the 7500 series. The receive access lists protect the device from harmful traffic before the traffic can impact the route processor. Receive path 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 CPU load is distributed to the line card processors and helps mitigate load on the main route processor. The white paper entitled "GSR: Receive Access Control Lists" will help identify and allow legitimate traffic to your device and deny all unwanted packets: <http://www.cisco.com/warp/public/707/racl.html>

- **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/warp/public/707/iacl.html>

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

☐ **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.

[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.

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

☐ **Status of This Notice: INTERIM**

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. CISCO EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE.

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 will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.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
- cisco-nsp@puck.nether.net
- full-disclosure@lists.netsys.com
- vulnwatch@vulnwatch.org
- comp.dcom.sys.cisco
- Various other mailing lists

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 1.5	2004-May-05	Updated software availability information for 12.0S, 12.1EB, 12.2, 12.2S, 12.2SW, 12.3, 12.3T, 12.3XH, 12.3XK, and 12.3XQ. No new releases added.
Revision 1.4	2004-April-29	In the Software Versions and Fixes section, modified the entry for 12.3XC.
Revision 1.3	2004-April-23	In the Affected Products section, listed each release on a separate line.
Revision 1.2	2004-April-23	In the Affected Products section, modified 4th paragraph, and updated list of releases. In the Software Versions and Fixes section, modified/added entries for 12.1EB, 12.1EO, 12.1EU, 12.2SW, 12.2ZQ, 12.2XE, 12.2XF
Revision 1.1	2004-April-22	In the Software Versions and Fixes section, added Optical products table, and updated IOS Release table. In the Affected Products section, added Catalyst and Optical products, and 12.1(20)EO.
Revision 1.0	2004-April-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>.

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)

Send