

[NEWS] Vulnerabilities in Cisco's SNMP Message Processing

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-04/0090.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/22/04

To: list@securiteam.com

Date: 22 Apr 2004 18:58:20 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Vulnerabilities in Cisco's SNMP Message Processing

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).

DETAILS

Affected 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.

Securiteam: [NEWS] Vulnerabilities in Cisco's SNMP Message Processing

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.

Note: The list below is not comprehensive; it is provided to help quickly identify some commonly used releases. Please see the Software Versions and Fixes section of this advisory for the complete IOS upgrade table.

- * 12.0(23)S4, 12.0(23)S5
- * 12.0(24)S4, 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)EO
- * 12.1(20)EW, 12.1(20)EW1
- * 12.1(20)EC, 12.1(20)EC1
- * 12.2(12g), 12.2(12h)
- * 12.2(20)S, 12.2(20)S1
- * 12.2(21), 12.2(21a)
- * 12.2(23)
- * 12.3(2)XC1, 12.3(2)XC2
- * 12.3(5), 12.3(5a), 12.3(5b)
- * 12.3(6)
- * 12.3(4)T, 12.3(4)T1, 12.3(4)T2, 12.3(4)T3
- * 12.3(5a)B
- * 12.3(4)XD, 12.3(4)XD1

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".

Securiteam: [NEWS] Vulnerabilities in Cisco's SNMP Message Processing

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>>
<http://www.cisco.com/warp/public/620/1.html>.

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.

Securiteam: [NEWS] Vulnerabilities in Cisco's SNMP Message Processing

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.

Impact:

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

Software Versions and Fixes:

For a list of affected versions and their fixes, see:

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

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 that 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

Securiteam: [NEWS] Vulnerabilities in Cisco's SNMP Message Processing

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 OutputIF
[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

Securiteam: [NEWS] Vulnerabilities in Cisco's SNMP Message Processing

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>>
<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 that 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>>
<http://www.cisco.com/warp/public/707/iacl.html>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:psirt@cisco.com>> Cisco Systems Product Security Incident Response Team.

The original article can be found at:

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

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.