

# Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco Catalyst 6000, 6500 Series, and Cisco 7600 Series NAM (Network Analysis Module) Vulnerability

<http://www.cisco.com/warp/public/707/cisco-amb-20070228-nam.shtml>

## Revision 1.0

For Public Release 2007 February 28 1600 UTC (GMT)

---

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

---

## Contents

[Cisco Response](#)

[Device-Specific Mitigation and Identification](#)

[Additional Information](#)

[Revision History](#)

[Cisco Security Procedures](#)

[Related Information](#)

---

## Cisco Response

### Vulnerability Characteristics

A vulnerability exists in Cisco Catalyst 6000 and 6500 series switches and Cisco 7600 series routers that have a Network Analysis Module (NAM; WS-SVC-NAM-1, WS-SVC-NAM-2, or WS-X6380-NAM) installed in the device chassis. Platforms running a vulnerable release of Cisco Internet Operating System (IOS) or Catalyst Operating System (Catalyst OS) software affected by this vulnerability can be exploited remotely by an unauthenticated attacker. Successful exploitation of this vulnerability may allow for complete control of the affected platform, which includes the ability to modify the device configuration. The attack vector used to exploit this vulnerability is through the Simple Network Management Protocol (SNMP) using UDP port 161 and spoofed SNMP packets. Spoofed SNMP packets will have a source IP address of the NAM installed in the affected device with a destination IP address configured on the affected

device. This vulnerability is not covered by a CVE ID.

This document contains information to assist Cisco customers in identifying and mitigating attempts to exploit the Cisco Catalyst 6000 and 6500 series and Cisco 7600 series NAM vulnerability. The vulnerability described in this document affects devices running Cisco IOS or Catalyst OS software and having a WS-SVC-NAM-1, WS-SVC-NAM-2, or WS-X6380-NAM installed in the platform.

Vulnerable, nonaffected, and fixed software information is available in the PSIRT Security Advisory at <http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml>.

## Mitigation Technique Overview

Cisco devices provide several countermeasures for the Cisco catalyst 6000 and 6500 series and Cisco 7600 series NAM vulnerability. Many of these protection methods should be considered general security best practices for infrastructure devices and the traffic that transits the network.

The most effective means of exploit prevention is provided by Cisco IOS software using the following:

- IP Source Guard
- Infrastructure Access Control Lists (iACLs)
- Transit Access Control Lists (tACLs)
- Unicast Reverse Path Forwarding (Unicast RPF)

These protection mechanisms filter, drop (discard), and verify the source IP address of packets trying to exploit the vulnerability described in this document. The most effective means of anti-spoofing protection against attacks with spoofed source IP addresses and spoofed source MAC addresses is provided through the proper deployment and configuration of Unicast RPF and IP source guard on the affected device.

The Cisco Intrusion Prevention System (IPS) provides detective and preventive controls for protection against attacks trying to exploit this vulnerability through the effective use of event-actions.

Detective controls can also be performed using Cisco IOS NetFlow, Cisco ASA 5500 Series Adaptive Security Appliance, Cisco PIX 500 Series Security Appliance, and the Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers through syslog messages and the counter values displayed in the output from **show** commands.

## Device-Specific Mitigation and Identification



**Caution:** The effectiveness of any mitigation technique is dependent on specific customer situations such as product mix, network architecture, traffic behavior, and organizational mission. As with any configuration change, evaluate the impact of this configuration prior to applying the change.

Specific information on mitigation and identification is available for these devices:

- [Cisco IOS Routers](#)

- [Cisco IOS Switches](#)
- [Cisco IOS NetFlow](#)
- [Cisco ASA, PIX, and FWSM Firewalls](#)
- [Cisco Intrusion Prevention System](#)

## Cisco IOS Routers

### Mitigation: Infrastructure Access Control Lists

In an effort to protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, infrastructure access control lists (iACLs) should be deployed to perform policy enforcement of traffic sent to infrastructure equipment. The construction of an iACL is accomplished by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. For maximum protection of infrastructure devices, iACLs deployed on Cisco IOS routers should be applied to all interfaces (where a Layer 3 IP address is configured) in the ingress direction.

In the following example, the address block 192.168.1.0/24 is the infrastructure address space, and 192.168.1.66 is the IP address configured on the NAM installed in the affected device. The iACL policy denies SNMP packets sourced from the IP address of the NAM installed in the affected device and SNMP packets sent to addresses that are part of the infrastructure address space. Care should be taken to allow required traffic for routing and administrative access prior to denying all traffic sent directly to infrastructure devices. Whenever possible, infrastructure address space should be distinct from the address space used for user and services segments. Using this addressing methodology will assist with the construction and deployment of iACLs.

Added access list entries (ACEs) should be implemented as part of an iACL policy that is used to filter traffic at network ingress points.

Additional information about iACLs is available at [Protecting Your Core: Infrastructure Protection Access Control Lists](#).

```
!-- Permit/Deny additional Layer3 and Layer4 traffic sent to the
!-- infrastructure address space in accordance with existing security
!-- policies and configurations. Deny all Simple Network Management
!-- Protocol (SNMP) packets on port UDP/161 sent to any IP address
!-- configured within the address block of 192.168.1.0/24, which is
!-- the infrastructure address space, except from known trusted source
!-- networks (ex: management networks, security operations center,
network
!-- operations center).
```

```
ip access-list extended infrastructure-acl-policy
```

```
!-- The following are vulnerability-specific access control entries
```

(ACEs)

*!-- to aid in identification of attacks.*

```
deny udp host 192.168.1.66 any eq 161
deny udp any 192.168.1.0 0.0.0.255 eq 161
```

*!-- Explicit deny ACE for traffic sent to addresses configured  
!-- within the infrastructure address space.*

```
deny ip any 192.168.1.0 0.0.0.255
```

*!-- Permit/Deny all other Layer3 and Layer4 traffic in accordance with  
!-- existing security policies and configurations.*

*!-- Apply iACL to interface(s) in the ingress direction.*

```
interface GigabitEthernet0/0
 ip address 192.168.1.254 255.255.255.0
 ip access-group infrastructure-acl-policy in
!
```

## **Mitigation: Anti-Spoof Protection Using Unicast Reverse Path Forwarding**




The vulnerability described in this document can be exploited by spoofed packets. Protection mechanisms for anti-spoofing exist through the proper deployment and configuration of Unicast Reverse Path Forwarding (Unicast RPF). Unicast RPF can detect and drop (discard) packets transiting through a router or switch that lack a verifiable IP source address. Unicast RPF should not be relied on to provide 100 percent protection because spoofed packets may still enter the network through a Unicast RPF-enabled interface for which there is a return route to the IP source address within the packet or allowed by anti-spoofing access-lists.

Strict mode Unicast RPF is most effective against spoofed attacks when properly deployed and configured on the affected device. Strict mode Unicast RPF coupled with IP source guard provides the most effective means of anti-spoofing protection for the vulnerability described in this document.

Care must be taken to ensure that the appropriate Unicast RPF mode (loose or strict) is configured during the deployment of this feature because it can drop legitimate traffic transiting through the network. Asymmetric traffic flows may be of concern when deploying this feature, and Unicast RPF loose mode is a scalable option for traffic of this type. However, loose mode Unicast RPF does not provide effective threat mitigation for this vulnerability.

Additional information about Unicast RPF is available at [Unicast Reverse Path Forwarding Loose Mode](#) and [Unicast Reverse Path Forwarding Enhancements for the Internet Service Provider \(ISP\)](#).

iACLs coupled with anti-spoofing protection mechanisms via Unicast RPF provide an added layer of threat mitigation for this vulnerability. iACL can also be used as a form of limited anti-spoofing protection by explicitly creating access control list entries (ACEs) that deny source addresses of the infrastructure IP address space.

There are Best Current Practices (BCPs) distributed through the [IETF](#)  that provide methods for limiting the risk and impact to the network and infrastructure from attacks that use spoofed source addresses. "Ingress Filtering for Multihomed Networks" ([BCP84](#) ) and "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing" ([BCP38](#) ) are the BCPs that provide information and suggestions regarding how to mitigate spoofing attacks.

## Identification: Infrastructure Access Control Lists

With an iACL, after the access list has been applied to an interface in the ingress direction, the **show ip access-lists** command identifies the number of SNMP packets on UDP port 161 that are being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit this vulnerability. An example output for **show ip access-lists infrastructure-acl-policy** follows:

```
router#show ip access-lists infrastructure-acl-policy
Extended IP access list infrastructure-acl-policy
 10 deny udp host 192.168.1.66 any eq 161 (192 matches)
 20 deny udp any 192.168.1.0 0.0.0.255 eq 161 (87 matches)
 30 deny ip any 192.168.1.0 0.0.0.255

--      Infrastructure ACL Policy Truncated      --
-- Permit/Deny other Layer3 and Layer4 traffic in --
-- accordance with existing security policies and --
-- configurations.                               --
router#
```

In the above example, access list *infrastructure-acl-policy* has dropped 192 UDP port 161 (SNMP) packets sourced from the IP address of the NAM installed in the affected device on ACE sequence ID 10 and 87 UDP port 161 (SNMP) packets on ACE sequence ID 20. This iACL is applied to interface GigabitEthernet0/0 in the ingress direction.

## Identification: Anti-Spoof Protection Using Unicast Reverse Path Forwarding

With Unicast RPF properly deployed and configured throughout the network infrastructure, the **show ip interface**, **show cef drop**, **show cef interface type slot/port internal**, and **show ip traffic** commands can be used to identify the number of packets that Unicast RPF has dropped (discarded).

```
router#show ip interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
 Internet address is 192.168.1.254/24
 Broadcast address is 192.168.1.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Multicast reserved groups joined: 224.0.0.10 224.0.0.5 224.0.0.6
```

```

Outgoing access list is not set
Inbound access list is infrastructure-acl-policy
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are never sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is enabled
IP CEF switching is enabled
IP Selective flow switching turbo vector
IP Flow CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, Flow cache, CEF, Subint Flow
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
IP verify source reachable-via RX, allow default, allow self-ping
18 verification drops
0 suppressed verification drops
router#
router#show cef drop
CEF Drop Statistics
Slot  Encap_fail  Unresolved  Unsupported      No_route      No_adj
ChkSum_Err
RP           158           0           0           18
0            0
router#
router#show cef interface GigabitEthernet 0/0 internal
GigabitEthernet0/0 is up (if_number 2)
Corresponding hwidb fast_if_number 2
Corresponding hwidb firstsw->if_number 2
Internet address is 192.168.1.254/24
ICMP redirects are never sent
Per packet load-sharing is disabled
IP unicast RPF check is enabled
Inbound access list is not set
Outbound access list is not set

```

```

Hardware idb is GigabitEthernet0/0
Fast switching type 1, interface type 27
IP CEF switching enabled
IP Selective flow switching turbo vector
IP Flow CEF switching turbo vector
Input fast flags 0x4000, Input fast flags2 0x8, Output fast flags
0x0, Output fast flags2 0x1
  ifindex 2(2)
Slot 0 Slot unit 0 Unit 0 VC -1
Transmit limit accumulator 0x0 (0x0)
IP MTU 1500
Subblocks:
  ip verify: via=rx (allow default), acl=0, drop=18, sdrop=0, allow
self-ping
router#
router#show ip traffic
IP statistics:
  Rcvd: 68051015 total, 2397325 local destination
        43999 format errors, 0 checksum errors, 33 bad hop count
        2 unknown protocol, 929 not a gateway
        21 security failures, 190123 bad options, 542768 with options
  Opts: 352227 end, 452 nop, 36 basic security, 1 loose source route
        45 timestamp, 59 extended security, 41 record route
        53 stream ID, 3 strict source route, 40 alert, 45 cipso, 0 ump
        361634 other
  Frags: 0 reassembled, 10008 timeouts, 56866 couldn't reassemble
        0 fragmented, 0 fragments, 0 couldn't fragment
  Bcast: 64666 received, 0 sent
  Mcast: 1589885 received, 2405454 sent
  Sent: 3001564 generated, 65359134 forwarded
  Drop: 4256 encapsulation failed, 0 unresolved, 0 no adjacency
        18 no route, 18 unicast RPF, 0 forced drop
        0 options denied
  Drop: 0 packets with source IP address zero
  Drop: 0 packets with internal loop back IP address

----- "show ip traffic" output truncated -----

router#

```

In the above examples, Unicast RPF has dropped 18 IP packets received on interface GigabitEthernet0/0 due to the inability to verify the source address of the IP packets within the Cisco Express Forwarding (CEF) Forwarding Information Base (FIB).

## Cisco IOS Switches

### Mitigation: Infrastructure Access Control Lists

In an effort to protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, infrastructure access control lists (iACLs) should be deployed to perform policy enforcement of traffic sent to

infrastructure equipment. The construction of an iACL is accomplished by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. For maximum protection of infrastructure devices, iACLs deployed on Cisco IOS switches should be applied to all interfaces (where a Layer 3 IP address is configured) in the ingress direction.

In the following example, the address block 192.168.1.0/24 is the infrastructure address space, and 192.168.1.66 is the IP address configured on the NAM installed in the affected device. The iACL policy denies SNMP packets sourced from the IP address of the NAM installed in the affected device and SNMP packets sent to addresses that are part of the infrastructure address space. Care should be taken to allow required traffic for routing and administrative access prior to denying all traffic sent directly to infrastructure devices. Whenever possible, infrastructure address space should be distinct from the address space used for user and services segments. Using this addressing methodology will assist with the construction and deployment of iACLs.

Added access list entries (ACEs) should be implemented as part of an iACL policy that is used to filter traffic at network ingress points.

Additional information about iACL is available at [Protecting Your Core: Infrastructure Protection Access Control Lists](#).

```
!-- Permit/Deny additional Layer3 and Layer4 traffic sent to the  
!-- infrastructure address space in accordance with existing security  
!-- policies and configurations. Deny all Simple Network Management  
!-- Protocol (SNMP) packets on port UDP/161 sent to any IP address  
!-- configured within the address block of 192.168.1.0/24, which is  
!-- the infrastructure address space, except from known trusted source  
!-- networks (ex: management networks, security operations center,  
network  
!-- operations center).
```

```
ip access-list extended infrastructure-acl-policy
```

```
!-- The following are vulnerability-specific access control entries  
(ACEs)  
!-- to aid in identification of attacks.
```

```
deny udp host 192.168.1.66 any eq 161  
deny udp any 192.168.1.0 0.0.0.255 eq 161
```

```
!-- Explicit default deny ACE for traffic sent to addresses configured  
!-- within the infrastructure address space.
```

```
deny ip any 192.168.1.0 0.0.0.255
```

```
!-- Permit/Deny all other Layer3 and Layer4 traffic in accordance with  
!-- existing security policies and configurations.
```

```
!-- Apply iACL to interface(s) in the ingress direction.
```

```
interface Vlan100
  ip address 192.168.1.254 255.255.255.0
  ip access-group infrastructure-acl-policy in
!
```

## Mitigation: Anti-Spoof Protection Using IP Source Guard

The vulnerability described in this document can be exploited by spoofed packets. Protection mechanisms for anti-spoofing exist through the proper deployment and configuration of IP source guard. IP source guard is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. IP source guard can be used to help prevent attacks from a malicious user who tries to spoof packets by forging the source IP address and/or the MAC address. When properly deployed and configured on the affected device, IP source guard coupled with strict mode Unicast RPF provides the most effective means of anti-spoofing protection for the vulnerability described in this document.

After IP source guard is enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping. A port access control list (PACL) is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic.

The IP source binding table has bindings that are learned by DHCP snooping or manually configured (static IP source bindings). An entry in this table has an IP address, its associated MAC address, and its associated VLAN number. The switch uses the IP source binding table only when IP source guard is enabled.

IP source guard is supported only on Layer 2 ports, including access and trunk ports. IP source guard can be configured for source IP address filtering or with source IP and MAC address filtering.

Additional information about IP source guard is available at [Configuring DHCP Features and IP Source Guard](#).

## Identification: Infrastructure Access Control Lists

With an iACL, after the access list has been applied to an interface in the ingress direction, the **show ip access-lists** command identifies the number of SNMP packets on UDP port 161 that are being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit this vulnerability. An example output for **show ip access-lists infrastructure-acl-policy** follows:

```
switch#show ip access-lists infrastructure-acl-policy
Extended IP access list infrastructure-acl-policy
 10 deny udp host 192.168.1.66 any eq 161 (65 matches)
 20 deny udp any 192.168.1.0 0.0.0.255 eq 161 (37 matches)
 30 deny ip any 192.168.1.0 0.0.0.255
--      Infrastructure ACL Policy Truncated      --
-- Permit/Deny other Layer3 and Layer4 traffic in --
```

```
-- accordance with existing security policies and --
-- configurations.                                --
switch#
```

In the above example, access list *infrastructure-acl-policy* has dropped 65 UDP port 161 (SNMP) packets sourced from the IP address of the NAM installed in the affected device on ACE sequence ID 10 and 37 UDP port 161 (SNMP) packets on ACE sequence ID 20. This iACL is applied to interface GigabitEthernet0/0 in the ingress direction.

**Note:** The counters displayed in the above output are for packets processed (dropped) in software. For hardware-based IOS switches, an additional command can be used to determine if packets are being dropped in hardware.

Starting with Cisco IOS Software Release 12.2(14)SX (for Supervisor 720) and release 12.2(17d)SXB (for Supervisor 2), the privileged EXEC command **show tcam interface vlan *vlan-id* acl {in|out} ip** provides ACE hit counts for packets that have been processed in hardware.

```
switch#show tcam interface vlan 100 acl in ip

* Global Defaults shared

Entries from Bank 0

Entries from Bank 1

deny      udp host 192.168.1.66 any eq snmp (131 matches)
deny      udp any 192.168.1.0 0.0.0.255 eq snmp (79 matches)
deny      ip any 192.168.1.0 0.0.0.255

--      Infrastructure ACL Policy Truncated      --
-- Permit/Deny other Layer3 and Layer4 traffic in --
-- accordance with existing security policies and --
-- configurations.                                --

switch#
```

In the above example, access list *infrastructure-acl-policy* has dropped 131 UDP port 161 (SNMP) packets sourced from the IP address of the NAM installed in the affected device in hardware and 79 UDP port 161 (SNMP) packets sent to addresses in the 192.168.1.0/24 address block in hardware for packets being sent through interface Vlan100, which is the infrastructure address space. This iACL is applied to interface Vlan100 in the ingress direction. The **show tcam interface vlan *vlan-id* acl {in|out} ip detail** command can optionally be used to display detailed information.

## Cisco IOS NetFlow

### Identification: Traffic Flow Identification Using NetFlow Records

Cisco IOS NetFlow can be configured on Cisco IOS routers and switches to aid in the identification of traffic flows that may be potential attempts to exploit the vulnerability described in this document. Packets should be investigated to determine whether they are attempts to exploit this vulnerability or to verify that the packets are legitimate traffic.

```
router#show ip cache flow
```



Total: 59957957 14.8 1 196 22.5  
 0.0 1.5

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP
<b>Gi0/0</b>	<b>192.168.1.201</b>	<b>Gi0/1</b>	<b>192.168.1.102</b>	<b>11</b>	<b>0984</b>
<b>00A1</b>					<b>1</b>
<b>Gi0/0</b>	<b>192.168.1.54</b>	<b>Gi0/1</b>	<b>192.168.1.158</b>	<b>11</b>	<b>0911</b>
<b>00A1</b>					<b>3</b>
Gi0/1	192.168.150.60	Gi0/0	10.89.16.226	06	0016
12CA					1
<b>Gi0/0</b>	<b>192.168.1.97</b>	<b>Gi0/1</b>	<b>192.168.1.28</b>	<b>11</b>	<b>0B3E</b>
<b>00A1</b>					<b>5</b>
<b>Gi0/0</b>	<b>192.168.1.17</b>	<b>Gi0/1</b>	<b>192.168.1.97</b>	<b>11</b>	<b>0B89</b>
<b>00A1</b>					<b>1</b>
Gi0/0	10.88.226.1	Gi0/1	192.168.202.22	11	007B
007B					1
<b>Gi0/0</b>	<b>192.168.1.185</b>	<b>Gi0/1</b>	<b>192.168.1.239</b>	<b>11</b>	<b>0BD7</b>
<b>00A1</b>					<b>1</b>
Gi0/0	10.89.16.226	Gi0/1	192.168.150.60	06	12CA
0016					1
<b>Gi0/0</b>	<b>192.168.1.250</b>	<b>Gi0/1</b>	<b>192.168.1.206</b>	<b>11</b>	<b>09B6</b>
<b>00A1</b>					<b>7</b>
Gi0/1	192.168.132.44	Gi0/0	10.89.245.149	11	007B
007B					1
<b>Gi0/0</b>	<b>192.168.1.243</b>	<b>Gi0/1</b>	<b>192.168.1.43</b>	<b>11</b>	<b>0A62</b>
<b>00A1</b>					<b>1</b>
<b>Gi0/0</b>	<b>192.168.1.228</b>	<b>Gi0/1</b>	<b>192.168.1.108</b>	<b>11</b>	<b>0BDB</b>
<b>00A1</b>					<b>2</b>
Gi0/0	192.168.208.63	Gi0/0	10.89.16.226	06	0016
1036					9
<b>Gi0/0</b>	<b>192.168.1.9</b>	<b>Gi0/1</b>	<b>192.168.1.171</b>	<b>11</b>	<b>0B20</b>
<b>00A1</b>					<b>1</b>
Gi0/0	192.168.208.63	Local	192.168.208.20	06	8291
0017					14
Gi0/1	192.168.202.22	Gi0/0	10.88.226.1	11	007B
007B					1
<b>Gi0/0</b>	<b>192.168.1.110</b>	<b>Gi0/1</b>	<b>192.168.1.163</b>	<b>11</b>	<b>092A</b>
<b>00A1</b>					<b>6</b>
<b>Gi0/0</b>	<b>192.168.1.230</b>	<b>Gi0/1</b>	<b>192.168.1.20</b>	<b>11</b>	<b>0C09</b>
<b>00A1</b>					<b>1</b>
Gi0/1	192.168.132.44	Gi0/0	64.101.128.56	11	C072
0035					2
<b>Gi0/0</b>	<b>192.168.1.131</b>	<b>Gi0/1</b>	<b>192.168.1.245</b>	<b>11</b>	<b>0B66</b>
<b>00A1</b>					<b>18</b>
<b>Gi0/0</b>	<b>192.168.1.7</b>	<b>Gi0/1</b>	<b>192.168.1.162</b>	<b>11</b>	<b>0914</b>
<b>00A1</b>					<b>1</b>
<b>Gi0/0</b>	<b>192.168.1.86</b>	<b>Gi0/1</b>	<b>192.168.1.27</b>	<b>11</b>	<b>0B7B</b>
<b>00A1</b>					<b>2</b>
Gi0/1	192.168.146.3	Gi0/0	192.168.156.100	2F	0000

```

0000      1
Gi0/0      64.101.128.56   Gi0/1      192.168.132.44   11 0035
C072      2
Gi0/0      192.168.1.86     Gi0/1      192.168.1.190    11 0ABC
00A1      2
Gi0/0      192.168.1.82     Gi0/1      192.168.1.31     11 095E
00A1      3
router#

```

In the above example, there are multiple flows for SNMP packets on UDP port 161 (hex value 00A1). This traffic is being sourced from and sent to addresses within the 192.168.1.0/24 address block, which is used for infrastructure devices. The packets for these flows may be spoofed and may indicate an attempt to exploit the vulnerability described in this document. These flows should be compared to baseline utilization for SNMP traffic sent on UDP port 161 and they should also be investigated to determine whether the flows are sourced from nontrusted host(s) and/or network(s).

```

router#show ip cache flow
IP packet size distribution (90784136 total packets):
  1-32  64  96  128  160  192  224  256  288  320  352  384  416
448  480
  .000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000
  512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
  .000 .001 .256 .000 .010 .000 .000 .000 .000 .000 .000

```

```

IP Flow Switching Cache, 4456704 bytes
  1885 active, 63651 inactive, 59960004 added
  129803821 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
  0 active, 16384 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never

```

Protocol	Total	Flows	Packets	Bytes	Packets	Active(Sec)
Idle(Sec)	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow
Flow						
TCP-Telnet	11393421	2.8	1	48	3.1	
0.0	1.4					
TCP-FTP	236	0.0	12	66	0.0	
1.8	4.8					
TCP-FTPD	21	0.0	13726	1294	0.0	
18.4	4.1					
TCP-WWW	22282	0.0	21	1020	0.1	
4.1	7.3					
TCP-X	719	0.0	1	40	0.0	
0.0	1.3					
TCP-BGP	1	0.0	1	40	0.0	0.0
15.0						

TCP-Frag	70399	0.0	1	688	0.0	0.0
22.7						
TCP-other	47861004	11.8	1	211	18.9	
0.0	1.3					
UDP-DNS	582	0.0	4	73	0.0	3.4
15.4						
UDP-NTP	287252	0.0	1	76	0.0	0.0
15.5						
UDP-other	310347	0.0	2	230	0.1	0.6
15.9						
ICMP	11674	0.0	3	61	0.0	19.8
15.5						
IPv6INIP	15	0.0	1	1132	0.0	0.0
15.4						
GRE	4	0.0	1	48	0.0	0.0
15.3						
Total:	59957957	14.8	1	196	22.5	
0.0	1.5					

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP
DstP Pkts					
<b>Gi0/0</b>	<b>192.168.1.201</b>	<b>Null</b>	<b>192.168.1.102</b>	<b>11</b>	<b>0984</b>
<b>00A1</b>					<b>1</b>
<b>Gi0/0</b>	<b>192.168.1.54</b>	<b>Null</b>	<b>192.168.1.158</b>	<b>11</b>	<b>0911</b>
<b>00A1</b>					<b>3</b>
Gi0/1	192.168.150.60	Gi0/0	10.89.16.226	06	0016
12CA					1
<b>Gi0/0</b>	<b>192.168.1.97</b>	<b>Null</b>	<b>192.168.1.28</b>	<b>11</b>	<b>0B3E</b>
<b>00A1</b>					<b>5</b>
<b>Gi0/0</b>	<b>192.168.1.17</b>	<b>Null</b>	<b>192.168.1.97</b>	<b>11</b>	<b>0B89</b>
<b>00A1</b>					<b>1</b>
Gi0/0	10.88.226.1	Gi0/1	192.168.202.22	11	007B
007B					1
<b>Gi0/0</b>	<b>192.168.1.185</b>	<b>Null</b>	<b>192.168.1.239</b>	<b>11</b>	<b>0BD7</b>
<b>00A1</b>					<b>1</b>
Gi0/0	10.89.16.226	Gi0/1	192.168.150.60	06	12CA
0016					1
<b>Gi0/0</b>	<b>192.168.1.250</b>	<b>Null</b>	<b>192.168.1.206</b>	<b>11</b>	<b>09B6</b>
<b>00A1</b>					<b>7</b>
Gi0/1	192.168.132.44	Gi0/0	10.89.245.149	11	007B
007B					1
<b>Gi0/0</b>	<b>192.168.1.243</b>	<b>Null</b>	<b>192.168.1.43</b>	<b>11</b>	<b>0A62</b>
<b>00A1</b>					<b>1</b>
<b>Gi0/0</b>	<b>192.168.1.228</b>	<b>Null</b>	<b>192.168.1.108</b>	<b>11</b>	<b>0BDB</b>
<b>00A1</b>					<b>2</b>
Gi0/0	192.168.208.63	Gi0/0	10.89.16.226	06	0016
1036					9
<b>Gi0/0</b>	<b>192.168.1.9</b>	<b>Null</b>	<b>192.168.1.171</b>	<b>11</b>	<b>0B20</b>
<b>00A1</b>					<b>1</b>
Gi0/0	192.168.208.63	Local	192.168.208.20	06	8291

```

0017      14
Gi0/1      192.168.202.22  Gi0/0      10.88.226.1    11 007B
007B      1
Gi0/0      192.168.1.110  Null      192.168.1.163  11 092A
00A1      6
Gi0/0      192.168.1.230  Null      192.168.1.20   11 0C09
00A1      1
Gi0/1      192.168.132.44  Gi0/0      64.101.128.56  11 C072
0035      2
Gi0/0      192.168.1.131  Null      192.168.1.245  11 0B66
00A1      18
Gi0/0      192.168.1.7   Null      192.168.1.162  11 0914
00A1      1
Gi0/0      192.168.1.86  Null      192.168.1.27   11 0B7B
00A1      2
Gi0/1      192.168.146.3  Gi0/0      192.168.156.100 2F 0000
0000      1
Gi0/0      64.101.128.56  Gi0/1      192.168.132.44  11 0035
C072      2
Gi0/0      192.168.1.86  Null      192.168.1.190  11 0ABC
00A1      2
Gi0/0      192.168.1.82  Null      192.168.1.31   11 095E
00A1      3

```

```
router#
```

```
router#show ip cef 192.168.1.0
```

```
192.168.200.0/24, version 322, epoch 0, cached adjacency 192.168.2.1
0 packets, 0 bytes
```

```
  via 192.168.2.1, GigabitEthernet0/1, 0 dependencies
```

```
    next hop 192.168.2.1, GigabitEthernet0/1
```

```
    valid cached adjacency
```

```
router#
```

```
router#show ip route 192.168.1.0
```

```
Routing entry for 192.168.1.0/24
```

```
  Known via "ospf 1", distance 110, metric 11, type intra area
```

```
  Last update from 192.168.2.1 on GigabitEthernet0/1, 09:09:07 ago
```

```
  Routing Descriptor Blocks:
```

```
    * 192.168.2.1, from 192.168.2.1, 09:09:07 ago, via GigabitEthernet0/1
```

```
      Route metric is 11, traffic share count is 1
```

```
router#
```

In the above example, there are multiple flows for SNMP packets on UDP port 161 (hex value 00A1). This traffic is being sourced from and sent to addresses within the 192.168.1.0/24 address block, which is used for infrastructure devices. The packets for these flows are spoofed and may indicate an attempt to exploit the vulnerability described in this document. The traffic associated with these flows is identified as spoofed packets because Unicast Reverse Path Forwarding (Unicast RPF) is enabled on the interfaces of this device and the egress interface value (*DstIf*) is *Null*. This traffic resulted in failure of the verification check for the source IP address within the packet because the 192.168.1.0/24 address block is reachable via GigabitEthernet0/1 based on the Cisco Express Forwarding (CEF) Forwarding Information Base (FIB) table. These packets were dropped (discarded) by the Unicast RPF feature and the flows should be investigated to determine the source of the spoofed traffic.

router#show ip cache flow

IP packet size distribution (90784136 total packets):

1-32	64	96	128	160	192	224	256	288	320	352	384	416	448	480
.000	.698	.011	.001	.004	.005	.000	.004	.000	.000	.003	.000	.000	.000	.000
512	544	576	1024	1536	2048	2560	3072	3584	4096	4608				
.000	.001	.256	.000	.010	.000	.000	.000	.000	.000	.000				

IP Flow Switching Cache, 4456704 bytes

1885 active, 63651 inactive, 59960004 added

129803821 aged polls, 0 flow alloc failures

Active flows timeout in 30 minutes

Inactive flows timeout in 15 seconds

IP Sub Flow Cache, 402056 bytes

0 active, 16384 inactive, 0 added, 0 added to flow

0 alloc failures, 0 force free

1 chunk, 1 chunk added

last clearing of statistics never

Protocol	Total	Flows	Packets	Bytes	Packets	Active(Sec)
Idle(Sec)						
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow
Flow						
TCP-Telnet	11393421	2.8	1	48	3.1	
0.0	1.4					
TCP-FTP	236	0.0	12	66	0.0	
1.8	4.8					
TCP-FTPD	21	0.0	13726	1294	0.0	
18.4	4.1					
TCP-WWW	22282	0.0	21	1020	0.1	
4.1	7.3					
TCP-X	719	0.0	1	40	0.0	
0.0	1.3					
TCP-BGP	1	0.0	1	40	0.0	0.0
15.0						
TCP-Frag	70399	0.0	1	688	0.0	0.0
22.7						
TCP-other	47861004	11.8	1	211	18.9	
0.0	1.3					
UDP-DNS	582	0.0	4	73	0.0	3.4
15.4						
UDP-NTP	287252	0.0	1	76	0.0	0.0
15.5						
UDP-other	310347	0.0	2	230	0.1	0.6
15.9						
ICMP	11674	0.0	3	61	0.0	19.8
15.5						
IPv6INIP	15	0.0	1	1132	0.0	0.0
15.4						
GRE	4	0.0	1	48	0.0	0.0

15.3

Total: 59957957 14.8 1 196 22.5

0.0 1.5

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP
Gi0/0 00A1	127.34.206.225	Gi0/1	192.168.1.102	11	0984
1					
Gi0/0 00A1	123.28.212.192	Gi0/1	192.168.1.158	11	0911
3					
Gi0/1 12CA	192.168.150.60	Gi0/0	10.89.16.226	06	0016
1					
Gi0/0 00A1	245.36.118.240	Gi0/1	192.168.1.28	11	0B3E
5					
Gi0/0 00A1	79.193.161.97	Gi0/1	192.168.1.97	11	0B89
1					
Gi0/0 007B	10.88.226.1	Gi0/1	192.168.202.22	11	007B
1					
Gi0/0 00A1	124.102.109.163	Gi0/1	192.168.1.239	11	0BD7
1					
Gi0/0 0016	10.89.16.226	Gi0/1	192.168.150.60	06	12CA
1					
Gi0/0 00A1	221.162.108.255	Gi0/1	192.168.1.206	11	09B6
7					
Gi0/1 007B	192.168.132.44	Gi0/0	10.89.245.149	11	007B
1					
Gi0/0 00A1	49.127.159.124	Gi0/1	192.168.1.43	11	0A62
1					
Gi0/0 00A1	113.47.245.213	Gi0/1	192.168.1.108	11	0BDB
2					
Gi0/0 1036	192.168.208.63	Gi0/0	10.89.16.226	06	0016
9					
Gi0/0 00A1	228.236.128.11	Gi0/1	192.168.1.171	11	0B20
1					
Gi0/0 0017	192.168.208.63	Local	192.168.208.20	06	8291
14					
Gi0/1 007B	192.168.202.22	Gi0/0	10.88.226.1	11	007B
1					
Gi0/0 00A1	108.110.92.234	Gi0/1	192.168.1.163	11	092A
6					
Gi0/0 00A1	216.28.179.117	Gi0/1	192.168.1.20	11	0C09
1					
Gi0/1 0035	192.168.132.44	Gi0/0	64.101.128.56	11	C072
2					
Gi0/0 00A1	92.187.97.206	Gi0/1	192.168.1.245	11	0B66
18					
Gi0/0 00A1	68.65.118.36	Gi0/1	192.168.1.162	11	0914
1					
Gi0/0 00A1	92.109.11.221	Gi0/1	192.168.1.27	11	0B7B
2					

```

Gi0/1      192.168.146.3   Gi0/0      192.168.156.100 2F 0000
0000      1
Gi0/0      64.101.128.56    Gi0/1      192.168.132.44  11 0035
C072      2
Gi0/0      255.141.201.158  Gi0/1      192.168.1.190   11 0ABC
00A1      2
Gi0/0      240.193.130.254  Gi0/1      192.168.1.31    11 095E
00A1      3
router#

```

In the above example, there are multiple flows for SNMP packets on UDP port 161 (hex value 00A1). The traffic is being sourced from random IP source addresses and sent to addresses within the 192.168.1.0/24 address block, which is used for infrastructure devices. The packets for these flows may be spoofed and may indicate an attempt to exploit the vulnerability described in this document. These flows should be compared to baseline utilization for SNMP traffic sent on UDP port 161 and they should also be investigated to determine whether the flows are sourced from nontrusted host(s) or network(s).

To view only the traffic for SNMP flows (UDP port 161; hex value 00A1), the command **show ip cache flow | include SrcIf|00A1** may be used to display these NetFlow records as shown here:

```

router#show ip cache flow | include SrcIf|00A1
SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr  SrcP
DstP  Pkts
Gi0/0      192.168.1.110     Gi0/1      192.168.1.163     11 092A
00A1      6
Gi0/0      192.168.1.230     Gi0/1      192.168.1.20      11 0C09
00A1      1
Gi0/1      192.168.132.44   Gi0/0      64.101.128.56    11 C072
0035      2
Gi0/0      192.168.1.131     Gi0/1      192.168.1.245     11 0B66
00A1      18
Gi0/0      192.168.1.7       Gi0/1      192.168.1.162     11 0914
00A1      1
Gi0/0      192.168.1.86      Gi0/1      192.168.1.27      11 0B7B
00A1      2
Gi0/1      192.168.146.3     Gi0/0      192.168.156.100  2F 0000
0000      1
Gi0/0      64.101.128.56    Gi0/1      192.168.132.44   11 0035
C072      2
Gi0/0      192.168.1.86      Gi0/1      192.168.1.190     11 0ABC
00A1      2
Gi0/0      192.168.1.82     Gi0/1      192.168.1.31      11 095E
00A1      3
router#

```

## Cisco ASA, PIX, and FWSM Firewalls

### Mitigation: Transit Access Control Lists

In an effort to protect the network from edge traffic that enters the network at ingress access points or traffic that transits the network, transit access control lists (tACLs) should be deployed to perform policy enforcement for this traffic. The construction of a tACL is accomplished by explicitly permitting only authorized traffic to enter the network at ingress access points or permitting authorized traffic to transit the network in accordance with existing security policies and configurations.

In the following example, the address block 192.168.1.0/24 is the infrastructure address space, and 192.168.1.66 is the IP address configured on the NAM installed in the affected device. The tACL policy denies unauthorized SNMP packets sourced from the IP address of the NAM installed in the affected device and SNMP packets sent to addresses that are part of the infrastructure address space.

Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic. Whenever possible, infrastructure address space should be distinct from the address space used for user and services segments. Using this addressing methodology will assist with the construction and deployment of tACLs.

Additional information about tACLs is available at [Transit Access Control Lists: Filtering at Your Edge](#).

```
!-- Permit/Deny additional Layer3 and Layer4 traffic un/authorized to  
enter  
!-- the network at ingress access points or traffic that has been un/  
authorized  
!-- to transit the network in accordance with existing security policies  
!-- and configurations. Deny all Simple Network Management Protocol  
(SNMP)  
!-- packets on port UDP/161 sent to any IP address configured within the  
!-- address block of 192.168.1.0/24, which is the infrastructure address  
!-- space, except from known trusted source networks (ex: management  
networks,  
!-- security operations center, network operations center).  
!  
!-- The following are vulnerability-specific access control entries  
(ACEs) to aid  
!-- in identification of attacks.  
  
access-list transit-acl-policy extended deny udp host 192.168.1.66 any  
eq 161  
access-list transit-acl-policy extended deny udp any 192.168.1.0  
255.255.255.0 eq 161  
  
!  
  
!-- Explicit default deny ACE for unauthorized traffic entering the  
network  
!-- at ingress access points or unauthorized transit traffic sent to  
addresses  
!-- configured within the infrastructure address space.  
  
access-list transit-acl-policy extended deny ip any 192.168.1.0
```

```
255.255.255.0
```

```
!
```

```
!-- Permit/Deny all other Layer3 and Layer4 traffic in accordance with  
!-- existing security policies and configurations.
```

```
!
```

```
!-- Apply tACL to interface(s) in the ingress direction.
```

```
access-group transit-acl-policy in interface outside
```

```
!
```

## Identification: Transit Access Control Lists

With a tACL, after the access list has been applied to an interface in the ingress direction, the **show access-list command** can be used to identify the number of SNMP packets on UDP port 161 that are being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit this vulnerability. An example output for **show access-list transit-acl-policy** follows:

```
firewall#show access-list transit-acl-policy  
access-list transit-acl-policy deny udp host 192.168.1.66 any eq snmp  
(hitcnt=154)  
access-list transit-acl-policy deny udp any 192.168.1.0 255.255.255.0  
eq snmp (hitcnt=119)  
access-list transit-acl-policy deny ip any 192.168.1.0 255.255.255.0  
(hitcnt=8)  
  
--          Transit ACL Policy Truncated          --  
-- Permit/Deny other Layer3 and Layer4 traffic in --  
-- accordance with existing security policies and --  
-- configurations.                                --  
firewall#
```

In the above example, access list transit-acl-policy has dropped 154 UDP port 161 (SNMP) packets sourced from the IP address of the NAM installed in the affected device and 119 UDP port 161 (SNMP) packets received from a nontrusted host or network. This tACL is applied to interface outside in the ingress direction. In addition, syslog message 106023 can provide valuable information, which includes the source and destination IP address, the source and destination port numbers, and the protocol for the denied packet.

## Identification: Firewall Syslog Messages

Firewall syslog message 106023 will be generated for packets denied by an ACE that does not have the **log** keyword present. Additional information about this syslog message is available at [Cisco Security Appliance System Log Message - 106023](#).

Information on configuring syslog for the Cisco ASA 5500 Series Adaptive Security Appliance or the Cisco PIX 500 Series Security Appliance is available at [Configuring Logging on the Cisco Security Appliance](#). Information on configuring syslog on the Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is available at [Configuring Monitoring and Logging on the Cisco FWSM](#).

In the following examples, the **show logging | grep** *regex* command is used to extract syslog messages from the logging buffer on the firewall. This is performed to obtain additional information about denied packets that could indicate potential attempts to exploit the vulnerability described in this document. It is possible to use different *regex* patterns with the **grep** keyword to search for specific data present within the logged messages.

```
firewall#show logging | grep 106023
Feb 21 2007 00:15:13: %ASA-4-106023: Deny udp src
outside:192.168.1.18/2944
    dst inside:192.168.1.191/161 by access-group "transit-acl-policy"
Feb 21 2007 00:15:13: %ASA-4-106023: Deny udp src
outside:192.168.1.200/2945
    dst inside:192.168.1.33/161 by access-group "transit-acl-policy"
Feb 21 2007 00:15:13: %ASA-4-106023: Deny udp src
outside:192.168.1.99/2946
    dst inside:192.168.1.240/161 by access-group "transit-acl-policy"
Feb 21 2007 00:15:13: %ASA-4-106023: Deny udp src
outside:192.168.1.100/2947
    dst inside:192.168.1.115/161 by access-group "transit-acl-policy"
Feb 21 2007 00:15:13: %ASA-4-106023: Deny udp src
outside:192.168.1.88/2949
    dst inside:192.168.1.38/161 by access-group "transit-acl-policy"
Feb 21 2007 00:15:13: %ASA-4-106023: Deny udp src
outside:192.168.1.175/2950
    dst inside:192.168.1.250/161 by access-group "transit-acl-policy"
firewall#
```

In the above example, the messages (106023) logged for tACL *transit-acl-policy* indicate potentially spoofed SNMP (UDP port 161) packets sent to the address block assigned to the network infrastructure. The syslog output in the following examples is representative of what the messages would look like on each of the Cisco ASA, PIX, and FWSM firewall platforms.

```
firewall#show logging | grep 192\.168\.1\.66
Feb 21 2007 00:15:14: %ASA-4-106023: Deny udp src
outside:192.168.1.66/2951
    dst inside:192.168.1.191/161 by access-group "transit-acl-policy"
Feb 21 2007 00:15:14: %ASA-4-106023: Deny udp src
outside:192.168.1.66/2952
    dst inside:192.168.1.13/161 by access-group "transit-acl-policy"
Feb 21 2007 00:15:14: %ASA-4-106023: Deny udp src
outside:192.168.1.66/2953
    dst inside:192.168.1.240/161 by access-group "transit-acl-policy"
Feb 21 2007 00:15:14: %ASA-4-106023: Deny udp src
outside:192.168.1.66/2954
    dst inside:192.168.1.13/161 by access-group "transit-acl-policy"
```

```
Feb 21 2007 00:15:14: %ASA-4-106023: Deny udp src
outside:192.168.1.66/2955
  dst inside:192.168.1.38/161 by access-group "transit-acl-policy"
Feb 21 2007 00:15:14: %ASA-4-106023: Deny udp src
outside:192.168.1.66/2956
  dst inside:192.168.1.13/161 by access-group "transit-acl-policy"
firewall#
```

In the above example, the messages (106023) logged for tACL *transit-acl-policy* indicate spoofed SNMP (UDP port 161) packets with a source IP address of the NAM installed in the affected device sent to the address block assigned to the network infrastructure. This traffic indicates an attempt to exploit the vulnerability in this document. The syslog output in the following examples is representative of what the messages would look like on each of the Cisco ASA, PIX, and FWSM firewall platforms.

Additional information about syslog messages for ASA and PIX security appliances is available at [Cisco Security Appliance System Log Messages](#). Additional information about syslog messages for the FWSM is available at [Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages](#).

## Cisco Intrusion Prevention System

### Mitigation: IPS Signature Event Actions

The Cisco Intrusion Prevention System (IPS) appliances and services modules can be used to provide threat detection and prevention against attempts to exploit the vulnerability described in this document. Starting with signature update S273 for sensors running Cisco IPS version 6.x or 5.x, the vulnerability described in this document in Cisco IOS can be detected by signature 5838/0 (Signature Name: Cisco IOS NAM SNMP Traffic) and in Catalyst OS can be detected by signature 5841/0 (Signature Name: CatOS NAM SNMP Traffic). Signatures 5838/0 and 5841/0 are both enabled by default and each trigger a *High* severity event (see the examples later in this section).

Cisco IPS sensors can be configured to perform an event action upon detection of an attack. The configured event action performs preventive or deterrent controls to help protect against an attack or attacks that are attempting to exploit the vulnerability described in this document. This vulnerability is exploited through the Simple Network Management Protocol (SNMP) using UDP on port 161 and can be successfully exploited using spoofed packets. Because UDP-based exploits can be easily spoofed, an attack or attacks that contain spoofed addresses may cause a configured event action that performs blocking capabilities through the construction and application of access control lists (ACLs) or by using the **shun** command to deny traffic from known trusted sources. Event actions that perform this type of controls are usually configured on sensors deployed in promiscuous mode. Because the traffic may be from known trusted sources, configured event actions that perform blocking should be set up for the short term only. This helps limit the amount of time the host(s) and or network(s) may be denied by an ACL or through the use of the **shun** command.

The most effective means of exploit prevention is provided by a Cisco IPS sensor deployed in inline protection mode through the use of an event action. Automatic Threat Prevention for Cisco IPS 6.x sensors deployed in inline protection mode provides threat prevention against an attack or attacks attempting to exploit this vulnerability. This is done through a default built-in override that performs an event action of **deny-packet-inline** for triggered signatures whose *riskRatingValue* range is 90 through 100. Additional information about the risk rating and the calculation of its value is available at [Cisco IPS Risk Rating Explained](#).

Cisco IPS 5.x sensors deployed in inline protection mode will need to have an event action configured on a per-signature

basis, using IPS signatures 5838/0 (Signature Name: Cisco IOS NAM SNMP Traffic) and 5841/0 (Signature Name: CatOS NAM SNMP Traffic), or an override can be configured to perform an event action for signatures that trigger and calculate the event(s) as a high-risk threat. Using the **deny-packet-inline** event action on sensors deployed in inline protection mode provides the most effective exploit prevention.

The following *High* severity events were triggered on a Cisco IPS sensor deployed in inline protection mode. The packet or packets associated with these events are denied (packet or packets are not transmitted) by the IPS sensor due to the event action **deny-packet-inline**. Note the presence of event action **deniedPacket: true** within the event output.

IPS signature 5838/0 (Signature Name: Cisco IOS NAM SNMP Traffic) triggers a *High* severity alarm on potential attempts to exploit the vulnerability described in this document, which may indicate an attempt to take complete control of the affected platform. The following *High* severity event was triggered by signature 5838/0 after a potential attempt to exploit this vulnerability in Cisco IOS.

```
sensor6x#show events alert | include id=5838
evIdsAlert: eventId=1166740638236368617 severity=high vendor=Cisco
originator:
  hostId: sensor6x
  appName: sensorApp
  appInstanceId: 32479
time: 2007/02/24 07:46:13 2007/02/24 01:46:13 CST
signature: description=Cisco IOS NAM SNMP Traffic id=5838 version=S273
  subsigId: 0
  sigDetails: Cisco IOS NAM SNMP Traffic
  marsCategory: Penetrate/GuessPassword/SNMP
  marsCategory: Penetrate/RemoteCmdExec/SNMP
  marsCategory: SANSTop20
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=IN 192.168.1.66
    port: 23932
  target:
    addr: locality=IN 192.168.1.13
    port: 161
  os: idSource=unknown relevance=unknown type=unknown
actions:
  deniedPacket: true
  riskRatingValue: targetValueRating=medium 95
  threatRatingValue: 60
  interface: ge0_0
  protocol: udp
sensor6x#
```

IPS signature 5841/0 (Signature Name: CatOS NAM SNMP Traffic) triggers a *High* severity alarm on potential attempts to exploit the vulnerability described in this document, which may indicate an attempt to take complete control of the affected platform. The following *High* severity event was triggered by signature 5841/0 after a potential attempt to exploit the vulnerability in Catalyst OS.

```
sensor6x#show events alert | include id=5841
evIdsAlert: eventId=1166740638236368710 severity=high vendor=Cisco
originator:
  hostId: sensor6x
  appName: sensorApp
  appInstanceId: 32479
time: 2007/02/24 08:15:52 2007/02/24 02:15:52 CST
signature: description=CatOS NAM SNMP Traffic id=5841 version=S273
  subsigId: 0
  sigDetails: CatOS NAM SNMP Traffic
  marsCategory: Penetrate/GuessPassword/SNMP
  marsCategory: Penetrate/RemoteCmdExec/SNMP
  marsCategory: SANSTop20
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=IN 192.168.1.66
    port: 64124
  target:
    addr: locality=IN 192.168.1.13
    port: 161
    os: idSource=unknown relevance=relevant type=unknown
actions:
  deniedPacket: true
  riskRatingValue: attackRelevanceRating=relevant
targetValueRating=medium 100
threatRatingValue: 65
interface: ge0_0
protocol: udp
sensor6x#
```

## Identification: IPS Signature Event Store

The following *High* severity events were triggered on a Cisco IPS sensor deployed in promiscuous mode. Note that the event action **deniedPacket: true** is not present.

IPS signature 5838/0 (Signature Name: Cisco IOS NAM SNMP Traffic) triggers a *High* severity alarm on potential attempts to exploit the vulnerability described in this document, which may indicate an attempt to take complete control of the affected platform. The following *High* severity event was triggered by signature 5838/0 after a potential attempt to exploit the vulnerability in Cisco IOS.

```
sensor6x#show events alert | include id=5838
evIdsAlert: eventId=1166740638236368428 severity=high vendor=Cisco
originator:
  hostId: sensor6x
  appName: sensorApp
  appInstanceId: 32479
time: 2007/02/24 07:24:33 2007/02/24 01:24:33 CST
signature: description=Cisco IOS NAM SNMP Traffic id=5838 version=S273
```

```
subsigId: 0
sigDetails: Cisco IOS NAM SNMP Traffic
marsCategory: Penetrate/GuessPassword/SNMP
marsCategory: Penetrate/RemoteCmdExec/SNMP
marsCategory: SANSTop20
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=IN 192.168.1.66
    port: 43489
  target:
    addr: locality=IN 192.168.1.13
    port: 161
    os: idSource=unknown relevance=unknown type=unknown
riskRatingValue: targetValueRating=medium 85
threatRatingValue: 85
interface: ge0_0
protocol: udp
sensor6x#
```

IPS signature 5841/0 (Signature Name: CatOS NAM SNMP Traffic) triggers a *High* severity alarm on potential attempts to exploit the vulnerability described in this document, which may indicate an attempt to take complete control of the affected platform. The following *High* severity event was triggered by signature 5841/0 after a potential attempt to exploit the vulnerability in Catalyst OS.

```
sensor6x#show events alert | include id=5841
evIdsAlert: eventId=1166740638236365783 severity=high vendor=Cisco
originator:
  hostId: sensor6x
  appName: sensorApp
  appInstanceId: 32479
time: 2007/02/24 07:24:34 2007/02/24 01:24:34 CST
signature: description=CatOS NAM SNMP Traffic id=5841 version=S273
  subsigId: 0
  sigDetails: CatOS NAM SNMP Traffic
  marsCategory: Penetrate/GuessPassword/SNMP
  marsCategory: Penetrate/RemoteCmdExec/SNMP
  marsCategory: SANSTop20
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=IN 192.168.1.66
    port: 37824
  target:
    addr: locality=IN 192.168.1.13
    port: 161
    os: idSource=unknown relevance=unknown type=unknown
riskRatingValue: targetValueRating=medium 85
```

```
threatRatingValue: 85
interface: ge0_0
protocol: udp
sensor6x#
```

## Additional Information

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.

## Revision History

Revision 1.0	2007-February-28	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](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>.

## Related Information

- [Protecting Your Core: Infrastructure Protection Access Control Lists](#)
  - [Transit Access Control Lists: Filtering at Your Edge](#)
  - [Unicast Reverse Path Forwarding Loose Mode](#)
  - [Unicast Reverse Path Forwarding Enhancements for the Internet Service Provider - Internet Service Provider Network Edge](#)
  - [Cisco IOS NetFlow - Home Page on Cisco.com](#)
  - [Cisco IOS NetFlow White Papers](#)
  - [Cisco Network Foundation Protection White Papers](#)
  - [Cisco Network Foundation Protection Presentations](#)
  - [Cisco Firewall Products - Home Page on Cisco.com](#)
  - [Cisco Intrusion Prevention System 6.x](#)
  - [Cisco IPS Risk Rating Explained](#)
  - [Cisco IPS 6.x Signature Downloads](#) ( [registered](#) customers only)
  - [Cisco IPS 5.x Signature Downloads](#) ( [registered](#) customers only)
  - [Cisco IPS Signatures by Release Version](#) ( [registered](#) customers only)
  - [Cisco IPS Signatures by Signature ID](#) ( [registered](#) customers only)
  - [Cisco Security Monitoring, Analysis, and Response System \(Cisco Security MARS\)](#)
-

## Help us help you.

### Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

### This document solved my problem.

- Yes
- No
- Just browsing

### Suggestions for improvement:

(256 character limit)

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)