

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)

Applied Mitigation Bulletins

# Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Catalyst 6500 and Cisco 7600 Series Devices Accessible via Loopback Address

<http://www.cisco.com/warp/public/707/cisco-amb-20070926-lb.shtml>

## Revision 1.0

For Public Release 2007 September 26 2200 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

This Applied Mitigation Bulletin is a companion document to the PSIRT Security Response *Catalyst 6500 and Cisco 7600 Series Devices Accessible via Loopback Address* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

## Vulnerability Characteristics

The Ethernet Out-of-Band Channel (EOBC) on Cisco Catalyst 6500 series switches and Cisco 7600 series routers allocates IP addresses from the 127.0.0.0/8 ([RFC 3330](#) , loopback) address range to intelligent services modules for internal communications. The IP addresses that are allocated from the 127.0.0.0/8 address range to the EOBC are accessible by devices outside of the affected system.

This vulnerability can be exploited remotely with or without authentication and without end-user interaction. Successful exploitation of this vulnerability can be used to bypass existing access control list filtering, cause a denial of service (DoS) condition for access via SSH or TELNET to the affected device using unauthenticated traffic, or allow access to intelligent services modules upon successful authentication. The attack vectors for exploitation are through a packet or packets using the ICMP, UDP, or TCP protocols. This vulnerability can be exploited via a layer 3 next hop adjacency or multiple hops through the use of Loose Source or Strict Source Route IP options. An attacker could exploit this vulnerability through spoofed packets. At the time of publication, there was no CVE name associated with this vulnerability.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Response, which is available at the following link: <http://www.cisco.com/warp/public/707/cisco-sr-20070926-lb.shtml>.

## Mitigation Technique Overview

Cisco devices provide several countermeasures for the Catalyst 6500 and Cisco 7600 series accessible via loopback address vulnerability. Administrators are advised to consider these protection methods as general security best practices for infrastructure devices and the traffic that transits the network.

Cisco IOS Software can provide effective means of exploit prevention using the following methods:

- Infrastructure access control lists (iACLs)
- Transit access control lists (tACLs)
- Unicast Reverse Path Forwarding (Unicast RPF)
- IP source guard (IPSG)

These protection mechanisms filter and drop, as well as verify the source IP address of, packets that are attempting to exploit the vulnerability described in this document.

The proper deployment and configuration of Unicast RPF provides the most effective means of protection against attacks that use packets with spoofed source IP addresses. Unicast RPF should be deployed as close to all traffic sources as possible.

The proper deployment and configuration of IPSG provides the most effective means of protection against attacks with spoofed source MAC addresses.

Effective means of exploit prevention can also be provided by the Cisco ASA 5500 Series Adaptive Security Appliance, the Cisco PIX 500 Series Security Appliance, and the Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers. Packets with a destination IP address in the 127.0.0.0/8 address range are dropped by default. This includes packets where Loose Source or Strict Source Route IP options are present.

Effective use of Cisco Intrusion Prevention System (IPS) event actions provides visibility into and protection against attacks that attempt to exploit this vulnerability.

Cisco IOS NetFlow can provide visibility into these exploitation attempts using flow records.

Cisco IOS Software, Cisco ASA, Cisco PIX security appliances, and FWSM firewalls can provide visibility through syslog messages and the counter values displayed in the output from **show** commands.

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can also provide visibility through queries and event reporting.

## Risk Management

Organizations should follow their standard risk evaluation and mitigation processes to determine the potential impact of this vulnerability. Triage refers to sorting projects and prioritizing efforts that are most likely to be successful. Cisco has provided documents that can help organizations develop a risk-based triage capability for their information security teams. [Risk Triage for Security Vulnerability Announcements](#) and [Risk Triage and Prototyping in Information Security Engagements](#) can help organizations develop repeatable security evaluation and response processes.

## Device Specific Mitigation and Identification



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

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

- [Cisco IOS Routers and Switches](#)
- [Cisco IOS NetFlow](#)
- [Cisco ASA, PIX, and FWSM Firewalls](#)
- [Cisco Intrusion Prevention System](#)
- [Cisco Security Monitoring, Analysis, and Response System](#)

### Cisco IOS Routers and Switches

#### Mitigation: Infrastructure Access Control Lists

In an effort to protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, administrators should deploy infrastructure access control lists (iACLs) to perform policy enforcement of traffic sent to infrastructure equipment. Administrators can construct an iACL by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. For the maximum protection of infrastructure devices, deployed iACLs should be applied in the ingress direction on all interfaces to which an IP address has been configured.

In the following example, the address block of 127.0.0.0/8 (loopback) is allocated to the EOBC. The iACL policy denies all ICMP, UDP, TCP, and all other IP packets sent to the 127.0.0.0/8 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.

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

```
ip access-list extended Infrastructure-ACL-Policy
!
!-- The following vulnerability-specific access control entries !-- (ACEs) can
aid in identification of attacks !
deny icmp any 127.0.0.0
0.255.255.255 deny udp any 127.0.0.0 0.255.255.255 deny tcp any 127.0.0.0
0.255.255.255
!!-- Explicit deny ACE for traffic sent to
addresses allocated to !-- the 127.0.0.0/8 (loopback) address space !

deny ip any 127.0.0.0 0.255.255.255
!!--
Permit/deny all other Layer 3 and Layer 4 traffic in accordance !-- with
existing security policies and configurations !!-- Apply iACL to interfaces in
the ingress direction
interface GigabitEthernet0/0 ip
access-group Infrastructure-ACL-Policy in

!
```

Note that filtering with an interface access list will elicit the transmission of ICMP unreachable messages back to the source of the filtered traffic. Generating these messages could have the undesired effect of increasing CPU utilization on the device. In Cisco IOS Software, ICMP unreachable generation is limited to one packet every 500 milliseconds by default. ICMP unreachable message generation can be disabled using the interface configuration command **no icmp unreachable**. ICMP unreachable rate limiting can be changed from the default using the global configuration command **ip icmp rate-limit unreachable interval-in-ms**.

### Mitigation: Transit Access Control Lists

In an effort to protect the network from traffic that enters the network at ingress access points, which may include Internet connection points, partner and supplier connection points, or VPN connection points, administrators should deploy transit access control lists (tACLs) to perform policy enforcement. Administrators can construct a tACL 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.

The tACL policy denies all ICMP, UDP, TCP, and all other IP packets sent to affected devices with a destination address in the 127.0.0.0/8 (loopback) address space. In the following example, 127.0.0.0/8 (loopback) is the network IP address space allocated to the EOBC and used by affected devices. Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic.

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

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

access-list 150 deny icmp any 127.0.0.0 0.255.255.255
```

```

access-list 150 deny udp any 127.0.0.0 0.255.255.255 access-list 150 deny tcp
any 127.0.0.0 0.255.255.255 access-list 150 deny ip any 127.0.0.0 0.255.255.255

!!-- Permit/deny all other Layer 3 and Layer 4 traffic in
accordance !-- with existing security policies and configurations !!--
Explicit deny for all other IP traffic !
access-list 150 deny
ip any any
!!-- Apply tACL to interfaces in the ingress
direction
interface GigabitEthernet0/0 ip access-group 150 in

!

```

Note that filtering with an interface access list will elicit the transmission of ICMP unreachable messages back to the source of the filtered traffic. Generating these messages could have the undesired effect of increasing CPU utilization on the device. In Cisco IOS Software, ICMP unreachable generation is limited to one packet every 500 milliseconds by default. ICMP unreachable message generation can be disabled using the interface configuration command **no icmp unreachable**. ICMP unreachable rate limiting can be changed from the default using the global configuration command **ip icmp rate-limit unreachable interval-in-ms**.

## Mitigation: Spoofing Protection

### Unicast Reverse Path Forwarding

The Catalyst 6500 and Cisco 7600 series accessible via loopback address vulnerability described in this document can be exploited by spoofed IP packets. Administrators can deploy and configure Unicast Reverse Path Forwarding (Unicast RPF) as a protection mechanism against spoofing.

Unicast RPF is configured at the interface level and can detect and drop packets that lack a verifiable source IP address. Administrators should not rely on Unicast RPF to provide 100 percent spoofing protection because spoofed packets may enter the network through a Unicast RPF-enabled interface if an appropriate return route to the source IP address exists. Administrators should take care 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 that is transiting the network. In an enterprise environment, Unicast RPF might be enabled at the Internet edge and the internal access layer on the user-supporting Layer 3 interfaces.

Additional information is available in the [Unicast Reverse Path Forwarding Loose Mode Feature Guide](#).

For additional information about the configuration and use of Unicast RPF, reference the [Understanding Unicast Reverse Path Forwarding](#) Applied Intelligence white paper.

### IP Source Guard

IP source guard (IPSG) is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering packets based on the DHCP snooping binding database and manually configured IP source bindings. Administrators can use IPSG to prevent attacks from an attacker who attempts to spoof packets by forging the source IP address and/or the MAC address. When properly deployed and configured, IPSG coupled with strict mode Unicast RPF provides the most effective means of spoofing

protection for the vulnerability described in this document.

Additional information about the deployment and configuration of IPSG is available in [Configuring DHCP Features and IP Source Guard](#).

### Identification: Infrastructure Access Control Lists

After the administrator applies the iACL to an interface, the **show ip access-lists** command will identify the number of ICMP, UDP, TCP, or IP packets with a destination IP address in the 127.0.0.0/8 address space that have been filtered on interfaces on which the iACL is applied. Administrators should investigate filtered packets to determine whether they are attempts to exploit this vulnerability. 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 icmp any 127.0.0.0
0.255.255.255 (71 matches) 20 deny udp any 127.0.0.0
0.255.255.255 (184 matches) 30 deny tcp any 127.0.0.0
0.255.255.255 (39 matches) 40 deny ip any 127.0.0.0
0.255.255.255 (56 matches) switch#
```

In the preceding example, the access list *Infrastructure-ACL-Policy* has dropped **71 ICMP** packets by access control entry (ACE) sequence ID 10, **184 UDP** packets by access control entry (ACE) sequence ID 20, **39 TCP** packets by access control entry (ACE) sequence ID 30, and **56 IP** packets by access control entry (ACE) sequence ID 40.

### Identification: Transit Access Control Lists

After the administrator applies the tACL to an interface, the **show ip access-lists** command will identify the number of ICMP, UDP, TCP, or IP packets with a destination IP address in the 127.0.0.0/8 address space that have been filtered. Administrators should investigate filtered packets to determine whether they are attempts to exploit this vulnerability. Example output for **show ip access-lists 150** follows:

```
router#show ip access-lists 150 Extended IP access
list 150 10 deny icmp any 127.0.0.0 0.255.255.255 (32 matches)
20 deny udp any 127.0.0.0 0.255.255.255 (69 matches) 30 deny
tcp any 127.0.0.0 0.255.255.255 (51 matches) 40 deny ip any
127.0.0.0 0.255.255.255 (19 matches) 50 deny ip any any
router#
```

In the preceding example, access list *150* has dropped **32 ICMP** packets by access control entry (ACE) sequence ID 10, **69 UDP** packets by access control entry (ACE) sequence ID 20, **51 TCP** packets by access control entry (ACE) sequence ID 30, and **19 IP** packets by access control entry (ACE) sequence ID 40.

### Identification: Access List Logging

The **log** or **log-input** access control list (ACL) option will cause packets that match specific ACEs to be logged. The **log-input** option enables logging of the ingress interface in addition to the packet source and destination IP addresses and ports.



**Caution:** Access control list logging can be very CPU intensive and must be used with extreme

caution. Factors that drive the CPU impact of ACL logging are log generation, log transmission, and process switching to forward packets that match log-enabled ACEs.

The CPU impact from ACL logging can be addressed in hardware on the Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers with Supervisor Engine 720 or Supervisor Engine 32 using optimized ACL logging. The **ip access-list logging interval *interval-in-ms*** command can limit the effects of process switching induced by ACL logging. The **logging rate-limit *rate-per-second* [except *loglevel*]** command limits the impact of log generation and transmission.

For additional information about the configuration and use of ACL logging, reference the [Understanding Access Control List Logging](#) Applied Intelligence white paper.

### Identification: Spoofing Protection Using Unicast Reverse Path

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

Note: The **show command | begin *regex*** and **show command | include *regex*** command modifiers are used in the following examples to minimize the amount of output that administrators need to parse to view the desired information. Additional information about command modifiers is available in the "[show command](#)" sections of the Cisco IOS Configuration Fundamentals Command Reference.

Note: **show cef interface *type slot/port internal*** is a hidden command that must be fully entered at the command-line interface. Command completion is not available for it.

```
router#show ip
interface GigabitEthernet 0/0 | begin verify

!-- CLI Output Truncated --
IP verify
source reachable-via RX 2989 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 27 0 0 13 0 0
router# router#show cef interface GigabitEthernet 0/0 internal |
include drop

!-- CLI Output Truncated --
ip verify:
via=rx, acl=0, drop=2989, sdrop=0 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
13 no route, 2989 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
```

```
!-- CLI Output Truncated --
```

```
router#
```

In the preceding examples, Unicast RPF has dropped **2989 IP packets** received globally on all interfaces with Unicast RPF configured because of the inability to verify the source address of the IP packets within the Cisco Express Forwarding Forwarding Information Base.

## Cisco IOS NetFlow

### Identification: Traffic Flow Identification Using NetFlow Records

Administrators can configure Cisco IOS NetFlow on Cisco IOS routers and switches to aid in the identification of traffic flows that may be attempts to exploit the vulnerability described in this document. Administrators should investigate flows to determine whether they are attempts to exploit this vulnerability.

**Note:** Traffic with a source or destination IP address in the 127.0.0.0/8 address range should not be considered legitimate and should always be investigated.

```
router#show
ip cache flow IP packet size distribution (2343M total packets): 1-32
64 96 128 160 192 224 256 288 320 352 384 416 448 480 .000 .998 .000 .000 .000
.000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
2560 3072 3584 4096 4608 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 4456704 bytes 16 active, 65520 inactive, 2263988108
added 493842408 aged polls, 0 flow alloc failures Active flows timeout in 2
minutes Inactive flows timeout in 60 seconds IP Sub Flow Cache, 402120 bytes 32
active, 16352 inactive, 233008920 added, 2263988108 added to flow 0 alloc
failures, 167546 force free 1 chunk, 90 chunks 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 3364799
1.2 1 43 1.3 0.1 6.7 TCP-FTP 2255835547 810.8 1 44 832.9 0.1 6.6 TCP-FTPD 5 0.0
1 46 0.0 0.0 26.0 TCP-WWW 4240326 1.5 2 53 4.2 9.2 12.6 TCP-SMTP 22 0.0 1 46
0.0 0.0 45.3 TCP-X 5 0.0 1 46 0.0 0.0 26.2 TCP-BGP 27 0.0 1 50 0.0 0.0 43.0
TCP-NNTP 28 0.0 1 51 0.0 0.0 37.4 TCP-other 330602 0.1 29 235 3.5 8.7 20.9
UDP-DNS 2928 0.0 2 69 0.0 3.5 54.0 UDP-NTP 133945 0.0 1 75 0.0 0.6 58.0
UDP-other 66043 0.0 5 167 0.1 33.5 32.6 ICMP 1079 0.0 32 63 0.0 32.3 35.4
IP-other 58 0.0 1 28 0.0 0.0 57.5 Total: 2263975414 813.8 1 44 842.2 0.1 6.6
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts Gi0/0
192.168.7.122 Gi0/0 127.0.0.107 06 6281 0017 4
Gi0/0 192.168.3.193 Null 127.0.0.218 11 4A0E 2644 8
Gi0/0 192.168.2.7 Null 127.0.0.132 01 0000 0800 11 Gi0/0
10.89.16.9 Gi0/1 192.168.150.60 06 0C47 0016 3 Gi0/0 192.168.208.63 Gi0/0
10.89.16.9 06 0016 0D61 1248 Gi0/0 192.168.2.126 Null 127.0.0.15 01
0000 0800 2
Gi0/0 192.168.2.65 Null 127.0.0.43 01 0000 0800 17 Gi0/0
10.88.226.1 Gi0/1 192.168.206.5 11 007B 007B 1 Gi0/0 192.168.208.63 Gi0/0
10.89.16.9 06 0016 0D5D 57 Gi0/0 192.168.1.67 Gi0/0 127.0.0.224 01 0000
0800 6
Gi0/0 192.168.7.141 Gi0/0 127.0.0.98 11 1160 536F 19
Gi0/0 192.168.5.148 Gi0/0 127.0.0.131 11 1515 2728 13
Gi0/0 192.168.6.171 Gi0/0 127.0.0.233 06 32C5 0017 2
Gi0/0 192.168.0.56 Gi0/0 127.0.0.204 11 711F 5445 1
Gi0/0 192.168.1.250 Gi0/0 127.0.0.57 01 0000 0800 21 Gi0/0
10.89.254.17 Gi0/1 192.168.150.65 01 0000 030D 1 Gi0/0 10.87.98.218 Gi0/1
```

```

192.168.130.41 06 C21A 01BB 118 Gi0/0 192.168.5.65 Gi0/0 127.0.0.41 01
0000 0800 17 Gi0/0 192.168.3.59 Null 127.0.0.242 06 0642 0017
9
Gi0/0 192.168.4.139 Gi0/0 127.0.0.141 01 0000 0800 11
Gi0/0 192.168.5.164 Gi0/0 127.0.0.31 06 E84D 0017 2
Gi0/0 192.168.2.82 Null 127.0.0.34 11 82A4 738D 19
Gi0/0 192.168.7.33 Gi0/0 127.0.0.245 06 E47C 0017 3 Gi0/0
192.168.208.63 Gi0/0 10.89.16.9 06 0016 0D63 306 Gi0/0 192.168.208.63 Local
192.168.208.20 06 B4F1 0017 1193 Gi0/0 192.168.2.239 Null 127.0.0.159
01 0000 0800 11
Gi0/0 192.168.4.248 Gi0/0 127.0.0.205 01 0000 0800 7
Gi0/0 192.168.6.65 Gi0/0 127.0.0.132 06 F231 0017 1
Gi0/0 192.168.0.67 Gi0/0 127.0.0.19 11 9E5E 4589 13
Gi0/0 192.168.6.140 Gi0/0 127.0.0.52 06 D0AB 0017 4
Gi0/0 192.168.5.155 Gi0/0 127.0.0.178 01 0000 0800 16
Gi0/0 192.168.3.136 Null 127.0.0.87 11 7CFC B5B1 10
Gi0/0 192.168.7.18 Gi0/0 127.0.0.199 06 DBF4 0017 2
Gi0/0 192.168.5.140 Gi0/0 127.0.0.148 01 0000 0800 18
Gi0/0 192.168.6.104 Gi0/0 127.0.0.238 01 0000 0800 22 Gi0/0
10.88.226.1 Gi0/1 192.168.128.21 11 007B 007B 1 Gi0/0 192.168.4.142
Gi0/0 127.0.0.10 01 0000 0800 11
Gi0/0 192.168.2.47 Null 127.0.0.190 06 8AB6 0017 1 Gi0/0
192.168.208.64 Null 192.168.208.255 11 0089 0089 3 router#

```

In the preceding example, there are multiple flows for **ICMP (protocol hex value 01, decimal value 1)**, **UDP (protocol hex value 11, decimal value 17)**, and **TCP (protocol hex value 06, decimal value 6)**. This traffic is sent to addresses within the 127.0.0.0/8 (loopback) address space. The packets in these flows may be spoofed and may indicate an attempt to exploit the vulnerability described in this document. Administrators should never see legitimate traffic with a source or destination address in in the 127.0.0.0/8 address range. The traffic in these flows should be investigated.

To view only the traffic flows for ICMP (protocol hex value 01), UDP (protocol hex value 11), or TCP (protocol hex value 06) packets sourced from or sent to an IP address in the 127.0.0.0/8 address range, the command **show ip cache flow | include SrcIf|127\..\*01\_** for ICMP, **show ip cache flow | include SrcIf|127\..\*11\_** for UDP, and **show ip cache flow | include SrcIf|127\..\*06\_** for TCP will display the related NetFlow records as shown here:

### Example Output for ICMP NetFlow Records

```

router#show ip cache flow | include SrcIf|127\..*01_
SrcIf SrcIPAddress DstIf DstIPAddress Pr SrcP DstP Pkts Gi0/0 192.168.2.7 Null
127.0.0.132 01 0000 0800 11 Gi0/0 192.168.2.126 Null 127.0.0.15 01 0000 0800 2
Gi0/0 192.168.2.65 Null 127.0.0.43 01 0000 0800 17 Gi0/0 192.168.1.67 Gi0/0
127.0.0.224 01 0000 0800 6 Gi0/0 192.168.1.250 Gi0/0 127.0.0.57 01 0000 0800 21
Gi0/0 192.168.5.65 Gi0/0 127.0.0.41 01 0000 0800 17 Gi0/0 192.168.4.139 Gi0/0
127.0.0.141 01 0000 0800 11 Gi0/0 192.168.2.239 Null 127.0.0.159 01 0000 0800
11 Gi0/0 192.168.4.248 Gi0/0 127.0.0.205 01 0000 0800 7 Gi0/0 192.168.5.155
Gi0/0 127.0.0.178 01 0000 0800 16 Gi0/0 192.168.5.140 Gi0/0 127.0.0.148 01 0000
0800 18 Gi0/0 192.168.6.104 Gi0/0 127.0.0.238 01 0000 0800 22 Gi0/0
192.168.4.142 Gi0/0 127.0.0.10 01 0000 0800 11 router#

```

### Example Output for UDP NetFlow Records

```

router#show ip cache flow | include SrcIf|127\..*11_
SrcIf SrcIPAddress DstIf DstIPAddress Pr SrcP DstP Pkts Gi0/0 192.168.3.193
Null 127.0.0.218 11 4A0E 2644 8 Gi0/0 192.168.7.141 Gi0/0 127.0.0.98 11 1160

```

```
536F 19 Gi0/0 192.168.5.148 Gi0/0 127.0.0.131 11 1515 2728 13 Gi0/0
192.168.0.56 Gi0/0 127.0.0.204 11 711F 5445 1 Gi0/0 192.168.2.82 Null
127.0.0.34 11 82A4 738D 19 Gi0/0 192.168.0.67 Gi0/0 127.0.0.19 11 9E5E 4589 13
Gi0/0 192.168.3.136 Null 127.0.0.87 11 7CFC B5B1 10 router#
```

## Example Output for TCP NetFlow Records

```
router#show ip cache flow | include SrcIf|127\..*06_
SrcIf SrcIPAddress DstIf DstIPAddress Pr SrcP DstP Pkts Gi0/0 192.168.7.122
Gi0/0 127.0.0.107 06 6281 0017 4 Gi0/0 192.168.6.171 Gi0/0 127.0.0.233 06 32C5
0017 2 Gi0/0 192.168.3.59 Null 127.0.0.242 06 0642 0017 9 Gi0/0 192.168.5.164
Gi0/0 127.0.0.31 06 E84D 0017 2 Gi0/0 192.168.7.33 Gi0/0 127.0.0.245 06 E47C
0017 3 Gi0/0 192.168.6.65 Gi0/0 127.0.0.132 06 F231 0017 1 Gi0/0 192.168.6.140
Gi0/0 127.0.0.52 06 D0AB 0017 4 Gi0/0 192.168.7.18 Gi0/0 127.0.0.199 06 DBF4
0017 2 Gi0/0 192.168.2.47 Null 127.0.0.190 06 8AB6 0017 1 router#
```

## Cisco ASA, PIX, and FWSM Firewalls

### Identification: Firewall Syslog Messages

Note: Packets with a destination IP address in the 127.0.0.0/8 address range are dropped by default. No configuration changes are required to enable this functionality.

Firewall syslog messages *106014* for ICMP, *106006* for UDP, *106001* for TCP, and *106010* for all other IP protocols, will be generated for denied packets if the destination IP address falls in the 127.0.0.0/8 address range and the firewall has a default route in its routing table. This includes packets with the presence of Loose Source or Strict Source Route IP options.

Firewall syslog message *110001* will be generated for packets if the destination IP address falls in the 127.0.0.0/8 address range and the firewall does not have a default route in the routing table. This syslog message will also be generated if there is no default route in the routing table and Unicast RPF is enabled on the firewall. These packets will be dropped by the firewall. This includes packets with the presence of Loose Source or Strict Source Route IP options.

Additional information about these syslog messages are available in [Cisco Security Appliance System Log Messages](#).

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

In the following example, the **show logging | grep regex** command extracts syslog messages from the logging buffer on the firewall. These messages provide additional information about denied packets that could indicate attempts to exploit the vulnerability described in this document. It is possible to use different regular expressions with the **grep** keyword to search for specific data in the logged messages.

Additional information about regular expression syntax is available in [Using the Command Line Interface](#).

```
firewall# show
logging | grep (106014|106006|106001|106010|110001).*127\. Sep 18 2007
```

```

10:36:14: %ASA-2-106006: Deny inbound UDP from 192.168.0.1/2989 to
127.0.0.10/161 on interface outside Sep 18 2007 10:36:48: %ASA-3-106014: Deny
inbound icmp src outside:192.168.0.1 dst outside:127.0.0.10 (type 8, code 0)
Sep 18 2007 10:37:32: %ASA-2-106001: Inbound TCP connection denied from
192.168.0.1/2989 to 127.0.0.10/23 flags SYN on interface outside Sep 18 2007
10:37:57: %ASA-3-106010: Deny inbound protocol 47 src outside:192.168.0.1 dst
outside:127.0.0.10 Sep 18 2007 10:38:33: %ASA-3-106010: Deny inbound protocol
50 src outside:192.168.0.1 dst outside:127.0.0.10 Sep 18 2007 11:08:01:
%ASA-6-110001: No route to 127.0.0.10 from 192.168.0.1 firewall#

```

In the preceding example, the logged messages show packets for ICMP, UDP, TCP, GRE (protocol number 47), and ESP (protocol number 50) sent to IP addresses in the 127.0.0.0/8 address range.

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

## Cisco Intrusion Prevention System

### Mitigation: Cisco IPS Signature Event Actions

Administrators can use the Cisco Intrusion Prevention System (IPS) appliances and services modules to provide threat detection and help prevent attempts to exploit the vulnerability described in this document. Potential exploitation of this vulnerability may be detected by the following signatures if Loose Source or Strict Source Route IP options are present:

- 1004/0 - IP options-Loose Source Route
- 1006/0 - IP options-Strict Source Route

#### 1004/0 - IP options-Loose Source Route

Starting with signature update S2 for sensors running Cisco IPS version 6.x or 5.x, the vulnerability described in this document can be detected by signature 1004/0 (Signature Name: IP options-Loose Source Route). Signature 1004/0 is not enabled by default, triggers a *High* severity event, has a signature fidelity rating (SFR) of 100, and is configured with a default event action of **produce-alert**. Signature 1004/0 fires when a single packet sent using Loose Source Route IP options is detected. Firing of this signature may indicate a potential exploit of the vulnerability described in this document.

#### 1006/0 - IP options-Strict Source Route

Starting with signature update S2 for sensors running Cisco IPS version 6.x or 5.x, the vulnerability described in this document can be detected by signature 1006/0 (Signature Name: IP options-Strict Source Route). Signature 1006/0 is enabled by default, triggers a *High* severity event, has an SFR of 100, and is configured with a default event action of **produce-alert**. Signature 1006/0 fires when a single packet sent using Strict Source Route IP options is detected. Firing of this signature may indicate a potential exploit of the vulnerability described in this document.

Administrators can configure Cisco IPS sensors to perform an event action when an attack is detected. The configured event action performs preventive or deterrent controls to help protect against an attack that is attempting to exploit the vulnerability described in this document.

The establishment of the three-way TCP handshake is required to exploit this vulnerability via the TCP attack vector, which reduces the possibility of successful attacks using spoofed IP addresses.

Because ICMP-based and UDP-based exploits can be easily spoofed, an attack that contains spoofed addresses may cause a configured event action to inadvertently deny traffic from trusted sources. Event actions that perform blocking through ACLs or the **shun** command are usually configured on sensors deployed in promiscuous mode.

Cisco IPS sensors are most effective when deployed in inline protection mode combined with 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 that is attempting to exploit this vulnerability. Threat prevention is achieved through a default override that performs an event action of **deny-packet-inline** for triggered signatures with a *riskRatingValue* greater than 90. Additional information about the risk rating and the calculation of its value is available in [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. Alternatively, administrators can configure an override that can perform an event action for any signatures that are triggered and are calculated 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.

## Identification: IPS Signature Events

### Signature: 1004/0 - IP options-Loose Source Route

```
sensor6x# show events alert | include id=1004
evIdsAlert: eventId=1184079309279111264 severity=high vendor=Cisco originator:
hostId: sensor6x appName: sensorApp appInstanceId: 19682 time: 2007/09/19
06:11:49 2007/09/19 01:11:49 CDT signature: description=IP options-Loose Source
Route id=1004 version=S2 subsigId: 0 marsCategory:
Info/UncommonTraffic/TCPIPOptions interfaceGroup: vs0 vlan: 0 participants:
attacker: addr: locality=OUT 192.168.0.1 port: 2989 target: addr: locality=OUT
127.0.0.10 port: 23 os: idSource=unknown relevance=relevant type=unknown
actions: denyPacketRequestedNotPerformed: true denyFlowRequestedNotPerformed:
true triggerPacket:
!-- triggerPacket Output Truncated
--
riskRatingValue: attackRelevanceRating=relevant
targetValueRating=medium 100 threatRatingValue: 100 interface: ge0_0 protocol:
tcp
```

### Signature: 1006/0 - IP options-Strict Source Route

```
sensor6x# show events alert | include id=1006
evIdsAlert: eventId=1184079309279111262 severity=high vendor=Cisco originator:
hostId: sensor6x appName: sensorApp appInstanceId: 19682 time: 2007/09/19
05:55:58 2007/09/19 00:55:58 CDT signature: description=IP options-Strict
Source Route id=1006 version=S2 subsigId: 0 marsCategory:
Info/UncommonTraffic/TCPIPOptions interfaceGroup: vs0 vlan: 0 participants:
attacker: addr: locality=OUT 192.168.0.1 port: 2989 target: addr: locality=OUT
127.0.0.10 port: 23 os: idSource=unknown relevance=relevant type=unknown
actions: denyPacketRequestedNotPerformed: true denyFlowRequestedNotPerformed:
true triggerPacket:
!-- triggerPacket Output Truncated
```

```
--  
riskRatingValue: attackRelevanceRating=relevant  
targetValueRating=medium 100 threatRatingValue: 100 interface: ge0_0 protocol:  
tcp
```

## Cisco Security Monitoring, Analysis, and Response System

### Identification: Cisco Security Monitoring, Analysis, and Response System Query Type and Keyword

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can query on events for the Catalyst 6500 and Cisco 7600 series accessible via loopback address vulnerability using a query type and keyword regex. Using a keyword of **NR-1004/0** for IPS signature 1004/0 (which was created to detect packets with the Loose Source Route IP option present) or a keyword of **NR-1006/0** for IPS signature 1006/0 (which was created to detect packets with the Strict Source Route IP option present) and a query type of **All Matching Event Raw Messages** on the Cisco Security MARS appliance will provide a report that lists the events created by IPS signatures 1004/0 and 1006/0.

The following screen shot shows the values used to query for events created by IPS signature 1004/0 (Signature Name: IP options-Loose Source Route) and IPS signature 1006/0 (Signature Name: IP options-Strict Source Route):

The screenshot shows the Cisco MARS Query/Reports interface. At the top, there are navigation tabs: SUMMARY, INCIDENTS, QUERY / REPORTS (selected), RULES, MANAGEMENT, ADMIN, and HELP. Below these is a status bar with 'Query', 'Batch Query', and 'Report' options, and a timestamp 'Sep 19, 2007 1:23:31 AM CDT'. A user information bar shows 'CS-MARS Standalone: R4-MARS v4.2' and 'Login: Administrator (pnadmin)'. There are 'View Cases' and 'New Case' buttons.

The main section is titled 'Query Event Data' with the instruction 'Click the cells below to change query criteria:'. Below this is a 'Query type' field set to 'Event Raw Messages ranked by Time, 0h:20m' with 'Edit' and 'Clear' buttons. A table below shows query criteria:

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	ANY	None	ANY	ANY

An 'Apply' button is located below the table. Below the table is a section titled 'Specify raw message keywords:' containing a table for defining keywords:

Open (	Search String	) Close	Operation	Highlight
<input type="checkbox"/>	NR-1004/0	<input type="checkbox"/>	OR	<input type="checkbox"/>
<input type="checkbox"/>	NR-1006/0	<input type="checkbox"/>	None	<input type="checkbox"/>
<input type="checkbox"/>		<input type="checkbox"/>	None	<input type="checkbox"/>
<input type="checkbox"/>		<input type="checkbox"/>	None	<input type="checkbox"/>
<input type="checkbox"/>		<input type="checkbox"/>	None	<input type="checkbox"/>
<input type="checkbox"/>		<input type="checkbox"/>	None	<input type="checkbox"/>

The first two rows of the 'Specify raw message keywords' table are highlighted with a red box. Below this table are 'Cancel' and 'Apply' buttons.

At the bottom of the page, there is a copyright notice: 'Copyright © 2003, 2006 Cisco Systems, Inc. All rights reserved.' and a breadcrumb trail: 'Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help :: Feedback'.

The following screen shot shows the query results for NR-1004/0 and NR-1006/0 created by the Cisco Security MARS appliance using a query type and keyword regex query.

**CISCO SYSTEMS**

SUMMARY INCIDENTS **QUERY / REPORTS** RULES MANAGEMENT ADMIN HELP

Query Batch Query Report Sep 19, 2007 1:13:16 AM CDT

QUERY / REPORTS | CS-MARS Standalone: R4-MARS v4.2 Login: Administrator (pnadmin) :: Logout :: Activate

View Cases New Case

Load Report as On-Demand Query with Filter

Select Group... Incident ID:

Select Report... Session ID:  Show Show

Query Event Data

Click the cells below to change query criteria:

Query type: Event Raw Messages ranked by Time, 0h:20m Edit Clear

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-1004/0 OR NR-1006/0	None	ANY	ANY

Save As Report Save As Rule Submit

Query Results

Event / Session / Incident ID	Event Type	Time	Reporting Device	Raw Message	Path / Mitigation	Tune
E:256005368, S:256005368	IP Source Route	Sep 19, 2007 1:11:49 AM CDT	R4-IPS4240a	192.168.0.1/2989 --> 127.0.0.10/23 TCP IP Source Route, Time:1190182309,Risk Rating:100,VLAN:0,Port List:23,Action:cid:denyPacketRequestedNotPerformed cid:denyFlowRequestedNotPerformed		False Positive Tuning
E:256004373, S:256004373	IP Source Route	Sep 19, 2007 12:55:58 AM CDT	R4-IPS4240a	192.168.0.1/2989 --> 127.0.0.10/23 TCP IP Source Route, Time:1190181358,Risk Rating:100,VLAN:0,Port List:23,Action:cid:denyPacketRequestedNotPerformed cid:denyFlowRequestedNotPerformed		False Positive Tuning
IP Source Route	Sep 19, 2007 1:11:49 AM CDT	R4-IPS4240a	192.168.0.1/2989 --> 127.0.0.10/23 TCP IP Source Route, Time:1190182309,Risk Rating:100,VLAN:0,Port List:23,Action:cid:denyPacketRequestedNotPerformed cid:denyFlowRequestedNotPerformed			
IP Source Route	Sep 19, 2007 12:55:58 AM CDT	R4-IPS4240a	192.168.0.1/2989 --> 127.0.0.10/23 TCP IP Source Route, NR-1006/0, Time:1190181358,Risk Rating:100,VLAN:0,Port List:23,Action:cid:denyPacketRequestedNotPerformed cid:denyFlowRequestedNotPerformed			

## 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-September-26	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

- [Cisco Applied Mitigation Bulletins](#)
- [Protecting Your Core: Infrastructure Protection Access Control Lists](#)
- [Transit Access Control Lists: Filtering at Your Edge](#)
- [Understanding Access Control List Logging](#)
- [Understanding Unicast Reverse Path Forwarding](#)
- [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](#)
- [Unicast Reverse Path Forwarding Loose Mode](#)
- [Unicast Reverse Path Forwarding Enhancements for the Internet Service Provider - Internet Service Provider Network Edge](#)
- [Cisco 6.x Intrusion Prevention System](#)
- [Cisco IPS Risk Rating Explained](#)
- [Cisco IPS 6.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](#)
- [Common Vulnerabilities and Exposures \(CVE\)](#) 

---

**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)

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 2006-2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).