

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Multiple Multicast Vulnerabilities in Cisco IOS Software

<http://www.cisco.com/warp/public/707/cisco-amb-20080924-multicast.shtml>

Revision 1.2

Last Updated 2008 October 14 2000 UTC (GMT)

For Public Release 2008 September 24 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

This Applied Mitigation Bulletin is a companion document to the PSIRT Security Advisory *Multiple Multicast Vulnerabilities in Cisco IOS Software* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

There are multiple vulnerabilities in Cisco IOS Protocol Independent Multicast component. The following subsections summarize these vulnerabilities:

Crafted PIM packets may cause an IOS device to reload vulnerability. This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may cause the affected device to crash. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through PIM packets using IP protocol 103. An attacker could exploit this vulnerability using spoofed packets.

This vulnerability has been assigned CVE identifier CVE-2008-3808.

GSR may crash when processing a malformed multicast packet vulnerability. This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may cause the affected device to crash. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through malformed multicast IP packets . An attacker could exploit this vulnerability using spoofed packets.

This vulnerability has been assigned CVE identifier CVE-2008-3809.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisory, which is available at the following link: <http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml>.

Mitigation Technique Overview

Cisco devices provide several countermeasures for these vulnerabilities. Administrators are advised to consider these protection methods to be general security best practices for infrastructure devices and the traffic that transits the network. This section of the document provides an overview of these techniques.

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

- Infrastructure access control lists (iACLs) (**Crafted PIM packets may cause an IOS device to reload vulnerability** only)
- 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 these vulnerabilities.

The proper deployment and configuration of Unicast RPF provides an 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 an effective means of protection against spoofing attacks at the access layer.

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 using the following:

- Transit access control lists (tACLs) (**Crafted PIM packets may cause an IOS device to reload vulnerability** only)
- Unicast RPF

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

For the **Crafted PIM packets may cause an IOS device to reload vulnerability**, Cisco IOS NetFlow can provide visibility into network-based exploitation attempts using flow records.

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

Effective use of Cisco Intrusion Prevention System (IPS) event actions provides visibility into and protection against attacks that attempt to exploit the **GSR may crash when processing a malformed multicast packet vulnerability**.

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can also provide visibility for the **GSR may crash when processing a malformed multicast packet vulnerability** through queries, and event reporting.

Risk Management

Organizations are advised to follow their standard risk evaluation and mitigation processes to determine the potential impact of these vulnerabilities. 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](#) 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.

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

Cisco IOS Routers and Switches

Mitigation: Infrastructure Access Control Lists

To protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, administrators are advised to 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. An iACL workaround cannot provide complete protection against this vulnerability

when the attack comes from a trusted source address.

The iACL policy denies unauthorized PIM packets on IP protocol 103 that are sent to affected devices. In the following example, 192.168.60.0/24 is the IP address space that is used by the affected devices and 192.168.100.1 is the IP address of the Rendezvous Point (RP), which is a trusted host that requires access to and from the affected PIM devices. If using the PIM Bootstrap Router feature (BSR), permit PIM to each of the candidate BSRs, in this example 192.168.100.2 and 192.168.100.3 are the candidate BSRs. 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 iACLs.

Note: PIM version 2 uses the multicast group 224.0.0.13 while legacy PIM version 1 uses 224.0.0.2. [PIM version 2](#) has been available since IOS 11.3 and Cisco strongly discourages the use of PIM version 1.

Note: In the case of Bootstrap router (BSR), additional ACEs will be required to allow traffic to each of the candidate BSR routers to permit traffic between the infrastructure address space and the IP address of the candidate BSR interface designated by the [bsr-candidate command](#). In the provided example 192.168.100.2 and 192.168.100.3 are candidate BSRs.

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

```
ip access-list extended Infrastructure-ACL-Policy

!
!-- When applicable, include explicit permit statements for trusted
!-- sources that require access on the vulnerable protocol
!-- The Rendezvous Point (RP) address is 192.168.100.1
!-- access to and from the RP needs to be permitted
!

permit pim host 192.168.100.1 192.168.60.0 0.0.0.255
permit pim 192.168.60.0 0.0.0.255 host 192.168.100.1

!
!-- Permit PIMv2 multicast segment traffic, packets have destination
of:
!-- 224.0.0.13 PIMv2, use 224.0.0.2 instead if using legacy PIMv1
!

permit pim 192.168.60.0 0.0.0.255 host 224.0.0.13

!
!-- Permit PIM unicast traffic between adjacent routers (TTL=1)
!

permit pim 192.168.60.0 0.0.0.255 192.168.60.0 0.0.0.255 ttl eq 1

!
!-- In case of BSR, permit PIM to each of the candidate BSR,
```

```

!-- In this example 192.168.100.2 and 192.168.100.3
!-- are the candidate BSRs.
!

permit pim host 192.168.100.2 192.168.60.0 0.0.0.255
permit pim 192.168.60.0 0.0.0.255 host 192.168.100.2
permit pim host 192.168.100.3 192.168.60.0 0.0.0.255
permit pim 192.168.60.0 0.0.0.255 host 192.168.100.3

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

deny pim any 192.168.60.0 0.0.0.255

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

deny ip any 192.168.60.0 0.0.0.255

!
!-- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations
!

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 ip unreachables**. 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 vulnerabilities that are 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 complete 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 are advised to 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 vulnerabilities that are 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 PIM packets on IP protocol 103 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:

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
 10 permit pim host 192.168.100.1 192.168.60.0 0.0.0.255
 20 permit pim 192.168.60.0 0.0.0.255 host 192.168.100.1
 30 permit pim 192.168.60.0 0.0.0.255 host 224.0.0.13
 40 permit pim 192.168.60.0 0.0.0.255 192.168.60.0 0.0.0.255 ttl eq 1
 50 permit pim host 192.168.100.2 192.168.60.0 0.0.0.255
 60 permit pim 192.168.60.0 0.0.0.255 host 192.168.100.2
 70 permit pim host 192.168.100.3 192.168.60.0 0.0.0.255
 80 permit pim 192.168.60.0 0.0.0.255 host 192.168.100.3
 90 deny pim any 192.168.60.0 0.0.0.255 (45 matches)
100 deny ip any 192.168.60.0 0.0.0.255
```

In the preceding example, access list *Infrastructure-ACL-Policy* has dropped **45 PIM** packets on **IP protocol 103** for access control list entry (ACE) line 90.

For additional information about investigating incidents using ACE counters and syslog events, reference the [Identifying Incidents Using Firewall and IOS Router Syslog Events](#) Applied Intelligence white paper.

Administrators can use Embedded Event Manager to provide instrumentation when specific conditions are met, such as ACE counter hits. The Applied Intelligence white paper [Embedded Event Manager in a Security Context](#) provides

additional details about how to use this feature.

Identification: Access List Logging

The **log** and **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.

For Cisco IOS Software, 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.

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.

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 Forwarding

With Unicast RPF properly deployed and configured throughout the network infrastructure, administrators can use the **show cef interface** *type slot/port internal*, **show ip interface**, **show cef drop**, 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 will 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.

```
router#show cef interface GigabitEthernet 0/0 internal | include drop
--      CLI Output Truncated      --
  ip verify: via=rx (allow default), acl=0, drop=11, sdrop=0
router#
```

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, allow default, allow self-ping
11 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           18
0           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
Frag:  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
-      CLI Output Truncated      --
router#

```

In the preceding **show cef drop** and **show ip traffic** examples, Unicast RPF has dropped **18 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 Forwarding Information Base of the Cisco Express Forwarding.

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 **Crafted PIM packets may cause an IOS device to reload** vulnerability. Administrators are advised to investigate flows to determine whether they are attempts to exploit the vulnerability or whether they are legitimate traffic flows.

```

router#show ip cache flow
IP packet size distribution (599597945 total packets):

```

```

1-32  64  96  128  160  192  224  256  288  320  352  384  416
448  480
.000 .994 .000 .000 .001 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
.000 .000 .000 .000 .001 .000 .000 .000 .000 .000 .000

```

```

IP Flow Switching Cache, 4456704 bytes
28 active, 65508 inactive, 998642 added
11499304 ager polls, 0 flow alloc failures
Active flows timeout in 2 minutes
Inactive flows timeout in 60 seconds

```

```

IP Sub Flow Cache, 402120 bytes
17 active, 16367 inactive, 124 added, 124 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	3216	0.0	15	47	0.0	4.1
31.0						
TCP-FTP	5	0.0	9	64	0.0	74.3
22.4						
TCP-WWW	7660	0.0	14	641	0.0	7.0
21.2						
TCP-SMTP	476	0.0	8	86	0.0	
6.1	9.8					
TCP-other	895034	0.6	9	259	6.2	
0.8	3.1					
UDP-DNS	3773	0.0	11	79	0.0	9.0
58.7						
UDP-NTP	41071	0.0	1	76	0.0	0.5
60.4						
UDP-TFTP	136	0.0	1	59	0.0	1.3
60.2						
UDP-Frag	1	0.0	2	1046	0.0	0.0
60.8						
UDP-other	21899	0.0	7	175	0.1	60.0
33.5						
ICMP	25343	0.0	23299	56	421.1	11.9
54.6						
IP-other	3	0.0	1	30	0.0	40.0
40.7						
Total:	998617	0.7	600	59	427.6	
2.5	7.9					

```

SrcIf          SrcIPAddress  DstIf          DstIPAddress   Pr SrcP
DstP  Pkts

```

```

Gi0/1          192.168.150.60  Local          192.168.206.20  01 0000
0303         25
Gi0/0          192.168.208.63  Null          192.168.116.151 06 0016
085B         82
Gi0/1        192.168.60.1    Local        192.168.100.1   67 0000
0000        1
Gi0/0          192.168.104.132 Gi0/1          192.168.150.60  06 1A29
CC10         12
Gi0/1          192.168.130.66  Gi0/0          192.168.217.126 06 05FD
0050         3
Gi0/1          192.168.146.4   Gi0/0          192.168.226.1   11 007B
007B         1
router#

```

In the preceding example, there is one flow for **PIM on IP protocol 103 (hex value 67)**.

Note: Most PIM packets between adjacent neighbor routers have TTL equal to 1, which prevent them from showing up in NetFlow records. The following IP PIM messages are originated with TTL > 1:

- Traffic between the RP and infrastructure devices.
- In the case of BSR, the candidate RP Advertisement PIM packets sent to the elected bootstrap router.

This traffic is sourced from and sent to addresses within the 192.168.60.0/24 address block, which is used for infrastructure devices and the RP. The packets in these flows may be spoofed and may indicate an attempt to exploit the **Crafted PIM packets may cause an IOS device to reload** vulnerability. Administrators are advised to compare these flows to baseline utilization for PIM traffic sent on IP protocol 103 and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

To view only the traffic flows for PIM packets on PIM packets on IP protocol 103 (hex value 67), the command **show ip cache flow | include SrcIf|_67_** will display the related NetFlow records as shown here:

```

router#show ip cache flow | include SrcIf|_67_
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr SrcP
DstP  Pkts
Gi0/1        192.168.128.3  Local        192.168.206.20  67 0000
0000        1
router#

```

Cisco ASA, PIX, and FWSM

Mitigation: Transit Access Control Lists

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 are advised to deploy 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. A tACL workaround cannot provide complete protection against the **Crafted PIM packets may cause an IOS device to reload** vulnerability when the attack comes from a trusted source address.

The tACL policy denies unauthorized PIM packets on IP protocol 103 that are sent to affected devices. In the following example, 192.168.60.0/24 is the IP address space that is used by the affected devices, the host at 192.168.100.1 is considered the RP that requires access to the affected devices. If using BSR, permit PIM to each of the candidate BSRs, In this example 192.168.100.2 and 192.168.100.3 are the candidate BSRs. 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](#).

```
!  
!-- Include any explicit permit statements for trusted sources  
!-- that require access on the vulnerable protocols  
!  
  
access-list tACL-Policy extended permit pim host 192.168.100.1  
192.168.60.0 255.255.255.0  
access-list tACL-Policy extended permit pim 192.168.60.0 255.255.255.0  
host 192.168.100.1  
  
!  
!-- In case of BSR, permit PIM to each of the candidate BSRs,  
!-- them to be elected. In this example 192.168.100.2 and 192.168.100.3  
!-- are the candidate BSRs.  
!  
  
access-list tACL-Policy extended permit pim host 192.168.100.2  
192.168.60.0 255.255.255.0  
access-list tACL-Policy extended permit pim 192.168.60.0 255.255.255.0  
host 192.168.100.2  
access-list tACL-Policy extended permit pim host 192.168.100.3  
192.168.60.0 255.255.255.0  
access-list tACL-Policy extended permit pim 192.168.60.0 255.255.255.0  
host 192.168.100.3  
  
!  
!-- The following vulnerability-specific access control entries  
!-- (ACEs) can aid in identification of attacks  
!  
  
access-list tACL-Policy extended deny pim any 192.168.60.0  
255.255.255.0  
  
!  
!-- 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 tACL-Policy extended deny ip any any
```

```
!  
!-- Apply tACL to interface(s) in the ingress direction  
!  
  
access-group tACL-Policy in interface outside
```

Mitigation: Spoofing Protection Using Unicast Reverse Path Forwarding

The vulnerabilities that are described in this document can be exploited by spoofed IP packets. Administrators can deploy and configure 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 complete 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. In an enterprise environment, Unicast RPF might be enabled at the Internet edge and at the internal access layer on the user-supporting Layer 3 interfaces.

For additional information about the configuration and use of Unicast RPF, reference the Cisco Security Appliance Command Reference for [ip verify reverse-path](#) and the [Understanding Unicast Reverse Path Forwarding](#) Applied Intelligence white paper.

Identification: Transit Access Control Lists

After the tACL has been applied to an interface, administrators can use the **show access-list** command to identify the number of PIM packets on IP Protocol 103 that have been filtered. Administrators are advised to investigate filtered packets to determine whether they are attempts to exploit the **Crafted PIM packets may cause an IOS device to reload** vulnerability. Example output for **show access-list tACL-Policy** follows:

```
show access-list tACL-Policy  
access-list tACL-Policy; 8 elements  
access-list tACL-Policy line 1 extended permit pim host 192.168.100.1  
192.168.60.0 255.255.255.0 (hitcnt=0)  
access-list tACL-Policy line 2 extended permit pim 192.168.60.0  
255.255.255.0 host 192.168.100.1 (hitcnt=0)  
access-list tACL-Policy line 3 extended permit pim host 192.168.100.2  
192.168.60.0 255.255.255.0 (hitcnt=0)  
access-list tACL-Policy line 4 extended permit pim 192.168.60.0  
255.255.255.0 host 192.168.100.2 (hitcnt=0)  
access-list tACL-Policy line 5 extended permit pim host 192.168.100.3  
192.168.60.0 255.255.255.0 (hitcnt=0)  
access-list tACL-Policy line 6 extended permit pim 192.168.60.0  
255.255.255.0 host 192.168.100.3 (hitcnt=0)  
access-list tACL-Policy line 7 extended deny pim any 192.168.60.0  
255.255.255.0 (hitcnt=10)  
access-list tACL-Policy line 8 extended deny ip any any (hitcnt=0)
```

In the preceding example, access list *tACL-Policy* has dropped **10 PIM** packets on **IP protocol 103** received from an untrusted host or network. 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 IP protocol for the denied packet.

Identification: Firewall Access List Syslog Messages

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

Information about configuring syslog for the Cisco ASA 5500 Series Adaptive Security Appliance or the Cisco PIX 500 Series Security Appliance is available in [Monitoring the Security Appliance - Configuring and Managing Logs](#).

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 potential attempts to exploit the vulnerabilities that is 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 [Creating a Regular Expression](#).

```
firewall#show logging | grep 106023
Aug 04 2008 02:29:18: %ASA-4-106023: Deny protocol 103 src
outside:192.168.208.63
      dst inside:192.168.1.100 by access-group "tACL-Policy"
Aug 04 2008 02:30:40: %ASA-4-106023: Deny protocol 103 src
outside:192.168.208.63
      dst inside:192.168.1.100 by access-group "tACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL *tACL-Policy* show potentially spoofed **PIM** packets for **IP protocol 103** sent to the address block assigned to the infrastructure devices.

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 System Log Messages](#).

For additional information about investigating incidents using syslog events, reference the [Identifying Incidents Using Firewall and IOS Router Syslog Events](#) Applied Intelligence white paper.

Identification: Spoofing Protection Using Unicast Reverse Path Forwarding

Firewall syslog message *106021* will be generated for packets denied by Unicast RPF. Additional information about this syslog message is available in [Cisco Security Appliance System Log Message 106021](#).

Information about configuring syslog for the Cisco ASA 5500 Series Adaptive Security Appliance or the Cisco PIX 500 Series Security Appliance is available in [Monitoring the Security Appliance Configuring and Managing Logs](#).

Information about configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is available in [Monitoring the Firewall Services Module](#)

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 potential attempts to exploit the vulnerabilities that are 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 [Creating a Regular Expression](#)

```
firewall#show logging | grep 106021
Aug 04 2008 02:37:51: %ASA-1-106021: Deny PIM reverse path check from
    192.168.150.1 to 192.168.1.2 on interface outside
Aug 04 2008 02:37:59: %ASA-1-106021: Deny PIM reverse path check from
    192.168.150.1 to 192.168.1.2 on interface outside
firewall#
```

The **show asp drop** command can also identify the number of packets that the Unicast RPF feature has dropped, as shown in the following example:

```
firewall#show asp drop frame rpf-violated
    Reverse-path verify failed                2
firewall#
```

In the preceding example, Unicast RPF has dropped **2 IP packets** received on interfaces with Unicast RPF configured. Absence of output indicates that the Unicast RPF feature on the firewall has not dropped packets.

For additional information about debugging accelerated security path dropped packets or connections, reference the Cisco Security Appliance Command Reference for [show asp drop](#).

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 **GSR may crash when processing a malformed multicast packet vulnerability** that is described in this document. Beginning with signature update S358 for sensors running Cisco IPS version 6.x or 5.x, the vulnerability can be detected by signature 6999/0 (Signature Name: Cisco PIM Multicast Denial of Service Attack). Signature 6999/0 is enabled by default, triggers a *Medium* severity event, has a signature fidelity rating (SFR) of 90, and is configured with a default event action of **produce-alert**.

Signature 6999/0 fires when a single packet sent using PIM protocol 103 is detected. Firing of this signature may indicate a potential exploit of the GSR may crash when processing a malformed multicast packet vulnerability.

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 that is described in this document.

Exploits that use spoofed IP addresses may cause a configured event action to inadvertently deny traffic from trusted sources.

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 the vulnerability that is described in this document. Threat prevention is achieved through a default override that performs an event action for triggered signatures with a *riskRatingValue* greater than 90.

Cisco IPS 5.x sensors that are deployed in inline protection mode require 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 an event action on sensors deployed in inline protection mode provides the most effective exploit prevention.

For additional information about the risk rating and threat rating calculation, reference [Risk Rating and Threat Rating: Simplify IPS Policy Management](#).

Identification: IPS Signature Events

Signature: 6999/0 Cisco PIM Multicast Denial of Service Attack

```
IPS#show events alert
evIdsAlert: eventId=1212728313148096667 severity=medium vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 18712
  time: 2008/09/25 22:17:29 2008/09/25 17:17:29 CDT
  signature: description=Cisco PIM Multicast Denial of Service Attack
id=6999 version=S358
  subsigId: 0
  sigDetails: Cisco PIM Multicast Denial of Service Attack
  marsCategory: DoS/NetworkDevice
  interfaceGroup: vs0
  vlan: 203

!
!-- Packet details removed
!

riskRatingValue: targetValueRating=medium 52
threatRatingValue: 52
interface: ge0_0
protocol: IP protocol 103
```

Cisco Security Monitoring, Analysis, and Response System

Identification: Cisco Security Monitoring, Analysis, and Response System Incidents

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can create incidents regarding events that are related to the **GSR may crash when processing a malformed multicast packet vulnerability** that is described in this document using IPS signature 6999/0 (Signature Name: Cisco PIM Multicast Denial of Service

AttackCisco). After the S358 dynamic signature update has been downloaded, using keyword **NR-6999/0** for IPS signature 3999/0 and a query type of **All Matching Events** on the Cisco Security MARS appliance will provide a report that lists the incidents created by the IPS signature.

Beginning with the 4.3.1 and 5.3.1 releases of Cisco Security MARS appliances, support for the Cisco IPS dynamic signature updates feature has been added. This feature downloads new signatures from Cisco.com or from a local web server, correctly processes and categorizes received events that match those signatures, and includes them in inspection rules and reports. These updates provide event normalization and event group mapping, and they also enable the MARS appliance to parse new signatures from the IPS devices.



Caution: If dynamic signature updates are not configured, events that match these new signatures appear as *unknown event type* in queries and reports. MARS will not include these events in inspection rules, thus incidents may not be created for potential threats or attacks that occur within the network.

By default, this feature is enabled but requires configuration. If it is not configured, the following Cisco Security MARS rule will be triggered:

System Rule: CS-MARS IPS Signature Update Failure

When this feature is enabled and configured, administrators can determine the current signature version downloaded by MARS by selecting **Help > About** and reviewing the *IPS Signature Version* value.

Additional information about and instructions for configuring dynamic signature updates are available for the Cisco Security MARS [4.3.1](#) and [5.3.1](#) releases.

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 1.2	2008-October-14	Workaround information update.
Revision 1.1	2008-September-26	Update with signature 6999/0 information.
Revision 1.0	2008-September-24	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-IP-URPF-MIB Support](#)
- [Cisco Applied Mitigation Bulletins](#)
- [Cisco Guide to Harden Cisco IOS Devices](#)
- [Cisco Security Center](#)
- [Understanding Cross-Site Scripting \(XSS\) Threat Vectors](#)
- [Cisco IOS NetFlow - Home Page on Cisco.com](#)
- [Cisco IOS NetFlow White Papers](#)
- [NetFlow Performance Analysis](#)
- [Cisco Network Foundation Protection White Papers](#)
- [Cisco Network Foundation Protection Presentations](#)
- [TTL Expiry Attack Identification and Mitigation](#)
- [A Security-Oriented Approach to IP Addressing](#)
- [Understanding Control Plane Protection](#)
- [Cisco Firewall Products - Home Page on Cisco.com](#)
- [Unicast Reverse Path Forwarding Enhancements for the Internet Service Provider](#)
- [Cisco 6.x Intrusion Prevention System](#)
- [Cisco IPS 6.x Signature Downloads](#)
- [Cisco IPS Signature Search Page](#)
- [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)



[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.](#)