

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Crafted IP Option Vulnerability

<http://www.cisco.com/warp/public/707/cisco-amb-20070124-crafted-ip-option.shtml>

Revision 1.1

Last Updated 2007 January 25 2000 UTC (GMT)

For Public Release 2007 January 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

Vulnerability Characteristics

The Crafted IP Option vulnerability can be exploited remotely with no authentication and no user interaction is necessary. Successful exploitation may allow the attacker to cause a Denial of Service (DoS) condition or may allow the attacker to execute arbitrary code. The attack vectors are an Internet Control Message Protocol (ICMP) type 8, type 13, type 15, type 17 packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. This vulnerability is not covered by a CVE ID.

This document contains information to assist Cisco customers in mitigating attempts to exploit this vulnerability.

Vulnerable, non-affected and fixed software information is available in the PSIRT Security

Advisory:

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml>

Mitigation Technique Overview

Cisco devices provide several countermeasures for the Crafted IP Option vulnerability. Many of these should be considered general security best practices. In most instances, an attack is more likely from the local broadcast domain; however, it is possible for a successful attack to traverse the Internet.

On Cisco IOS platforms, the **drop** option of feature [IP Options Selective Drop](#) provides the most effective mitigation for this vulnerability. The draw back is that devices with this feature configured will drop all packets with IP Options, legitimate or otherwise. If IP Options are used in the network, the feature [Control Plane Policing](#) can offer an acceptable level of mitigation, especially on platforms and code trains that include [ACL Support for Filtering IP Options](#). In the absence of **IP Options Selective Drop** and **CoPP**, interface access-lists can also be used as a mitigation technique.

On Cisco PIX Security Appliances, Cisco ASA Adaptive Security Appliances, and Firewall Service Modules (FWSM) for Cisco Catalyst 6500 Switches and Cisco 7600 Routers, packets with IP Options are dropped by default which offers effective mitigation for this vulnerability.

All of these features are detailed in the Device Specific Mitigation and Identification section below.

Device-Specific Mitigation and Identification

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

- [Cisco Catalyst 6500 IOS Switch](#)
- [Cisco Catalyst 2960 Switch](#)
- [Cisco IOS Router](#)
- [Cisco PIX/ASA/FWSM Firewalls](#)
- [Cisco IOS XR Router](#)
- [Cisco Intrusion Prevention System \(IPS\)](#)
- [Cisco Security MARS \(CS MARS\)](#)

Cisco Catalyst 6500 IOS Switch



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.

Mitigation

Control Plane Policing: IOS software versions 12.2 SXD and later support **Control Plane Policing (CoPP)** which should be configured to help protect the device from attacks that target the management and control planes. This vulnerability uses IP Options as the exploitation vector and because of the way the switch processes IP Options, CoPP will protect the device on which it is configured, as well as down stream devices. All packets with IP Options either sent to this device or transiting through the device will be punted to the processor which results in CoPP filtering them. This applies to all platforms except the Cisco 12000 (GSR) where only packets containing IP Options destined for the router itself will be filtered.

The Cisco Security Advisory lists a specific set of seven IP protocols, ICMP types, and a TCP service that can be used to exploit the vulnerability. CoPP should be configured to deny all of these traffic types. Permitting any one of the seven types may leave the device at risk of exploitation. In the CoPP example below, the ACL entries that match the exploit packets with the permit action will be discarded by the policy-map drop function, while packets that match a deny action (not shown) are not affected by the policy-map drop function.

```
access-list 100 permit icmp any any echo
access-list 100 permit icmp any any information-request
access-list 100 permit icmp any any timestamp-request
access-list 100 permit icmp any any mask-request
access-list 100 permit tcp any any eq 465
access-list 100 permit 103 any any
access-list 100 permit 113 any any

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

class-map match-all drop-options-class
  match access-group 100

!
!

policy-map drop-options-policy
  class drop-options-class
    police 32000 1500 1500 conform-action drop exceed-action drop

!

control-plane
  service-policy input drop-options-policy
```

The packets dropped in the CoPP example above will impact all PIMv2-based multicast networking and all ICMP echo packets directed to the switch itself. CoPP will be applied only to transit ICMP echo packets with IP options set. All other transit ICMP echo packets will pass normally.

If the switch must process PIMv2 packets, the access-list entry for IP protocol 103 (**access-list 100 permit 103 any any**) can be removed from the CoPP access-list 100 and instead interface access-lists can be used to deny PIMv2 packets that are not sourced from or destined to legitimate internal multicast IP addresses. This would still allow spoofed PIMv2 packets to exploit this vulnerability and is not a complete workaround. The interface access-lists would need to be applied to all layer 3 physical interfaces and all VLAN interfaces on the switch.

Anti-Spoofing: This vulnerability can be exploited by a single, easily spoofed packet. Anti-spoof protection in the form of interface access-lists or unicast Reverse Path Forwarding can provide limited mitigation if properly configured. This mitigation should not be relied upon to provide 100% mitigation since spoofed packets may still enter the core from the interface expected by uRPF or allowed by anti-spoofing access-lists. Also care must be taken to ensure that the appropriate uRPF mode (loose or strict) is configured to ensure that legitimate packets are not dropped.

Additional information about unicast Reverse Path Forwarding is available at:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ft_urpf.html

Identification

Control Plane Policing: Once the CoPP configuration is deployed, the commands **show access-list 100** and **show policy-map control-plane all** can be used to identify packets dropped by the CoPP policy. Additionally SNMP queries using the **Cisco QoS MIB CISCO-CLASS-BASED-QOS-MIB** can be used to track packets being dropped by CoPP. Packets being dropped by CoPP should be investigated to determine if they are attempts to exploit the vulnerability.

Example output for **show access-list 100**:

```
6509-Switch#show access-list 100
Extended IP access list 100
 10 permit icmp any any echo (40 matches)
 20 permit icmp any any information-request
 30 permit icmp any any timestamp-request
 40 permit icmp any any mask-request
 50 permit tcp any any eq 465
 60 permit pim any any (966 matches)
 70 permit 113 any any
```

In the above example 40 ICMP echo packets and 966 PIM packets that were either destined to the switch itself or that contained IP Options have been dropped by the access-list associated with CoPP.

Example output for **show policy-map control-plane all**:

```
6509-Switch#show policy-map control-plane all

Control Plane Interface

Service-policy input: drop-options-policy

Hardware Counters:

class-map: drop-options-class (match-all)
 Match: access-group 100
 police :
  32000 bps 1000 limit 1000 extended limit
 Earl in slot 7 :
  570792 bytes
  5 minute offered rate 816 bps
  aggregate-forwarded 1020 bytes action: drop
  exceeded 569772 bytes action: drop
  aggregate-forward 0 bps exceed 816 bps

Software Counters:

Class-map: drop-options-class (match-all)
 394 packets, 26084 bytes
```

```

5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group 100
police:
  32000 bps, 1500 limit, 1500 extended limit
  conformed 394 packets, 26084 bytes; action: drop
  exceeded 0 packets, 0 bytes; action: drop
  violated 0 packets, 0 bytes; action: drop
  conformed 0 bps, exceed 0 bps, violate 0 bps

Class-map: class-default (match-any)
  33323 packets, 5544054 bytes
  5 minute offered rate 6000 bps, drop rate 0 bps
  Match: any

```

In the above example class-map **drop-options-class** has dropped 569772 bytes via the exceeded policy in hardware and 26084 bytes in software.

Example output for an SNMP query using the **Cisco QoS MIB CISCO-CLASS-BASED-QOS-MIB**.

```

Linux# tinsynmpget 10.89.236.151 ha5d7ogu355 1.3.6.1.4.1.9.9.166.1.15.1.1.16

1.3.6.1.4.1.9.9.166.1.15.1.1.16.1083.1085 = Counter32 569772

```

The output of this SNMP query matches the exceeded bytes that were dropped shown in the CLI output above for class-map: **drop-options-class**

1.3.6.1.4.1.9.9.166.1.15.1.1.16 is object **cbQosCMDropByte**.

1083.1085 is the table index number for a specific control-plane service policy class-map. The table index can be determined by SNMP walking OID: **1.3.6.1.4.1.9.9.166.1**. In this case **1083.1085** indicates class map **drop-options-class**.

Cisco Catalyst 2960 Switch



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.

Mitigation

Interface Access-lists: Fixed configuration switches can deploy layer 3 access-lists on their Management VLAN interfaces. The following ACL is specifically designed to block attack traffic and should be applied to the VLAN interface used to manage the switch.

```

access-list 150 deny icmp any any echo
access-list 150 deny icmp any any information-request
access-list 150 deny icmp any any timestamp-request
access-list 150 deny icmp any any mask-request
access-list 150 deny tcp any any eq 465
access-list 150 deny 103 any any
access-list 150 deny 113 any any

```

```
!-- Permit/deny all other IP traffic in accordance with
!-- existing security policies and configurations.
```

```
interface Vlan2
 ip address 10.1.50.1 255.255.255.0
 ip access-group 150 in
```

Identification

Interface Access-lists: Once the interface access-list is deployed, the command **show access-list 150** can be used to identify packets it is dropping. Dropped packets should be investigated to determine if they are attempts to exploit the vulnerability.

Example output for **show access-list 150**:

```
Access-2960#show access-list 150
Extended IP access list 150
 deny icmp any any echo (1706 matches)
 deny icmp any any information-request
 deny icmp any any timestamp-request
 deny icmp any any mask-request
 deny tcp any any eq 465
 deny pim any any
 deny 113 any any
```

In the above example 1706 ICMP echo packets destined to the switch itself have been dropped by the access-list configured on interface Vlan 2.

Cisco IOS Router



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.

Mitigation

IP Options Selective Drop: This feature is available beginning in Cisco IOS software version 12.0(23)S for Cisco 12000 (GSR), 12.0(32)S for 10720, and 12.3(4)T, 12.2(25)S, and 12.2(27)SBC for other routing devices.

IP Options Selective Drop drops all packets containing IP options and prevents them from targeting the receiving router and other devices downstream from the receiving router. The feature drops the packets in the packet input path before they are punted to the processor which minimizes the performance impact on the device. This also allows the router to drop packets with IP options at speeds and performance levels comparable to using interface access-lists to drop packets.

Deploying this command will drop legitimate packets containing IP options as well. Protocols this may impact include RSVP (used by Microsoft NetMeeting), MPLS TE, MPLS OAM, DVMRP, IGMPv3, IGMPv2, and legitimate PGM. This should be less of a concern at the Enterprise Internet edge where these services are less likely to be used.

Note: The **ignore** option of the global command **ip options ignore** is NOT a workaround for this issue.

Additional information about **IP Options Selective Drop** is available at:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/sel_drop.html

This command is enabled in global configuration mode by entering the following command:

```
Edge-Router(config)#ip options drop
```

After the command is enabled, the router will respond with the following warning at the CLI:

```
% Warning: RSVP and other protocols that use IP Options packets may not func
```

Control Plane Policing: The router's CoPP configuration should also be updated to account for packets that can be used to exploit this vulnerability. CoPP could also be used instead of **ip options drop** if legitimate packets with IP Options are required to traverse the Enterprise Edge to the Internet.

```
ip access-list extended drop-affected-options
 permit icmp any any echo option any-options
 permit icmp any any information-request option any-options
 permit icmp any any timestamp-request option any-options
 permit icmp any any mask-request option any-options
 permit pim any any option any-options
 permit 113 any any option any-options
 permit tcp any any eq 465 option any-options
```

```
!-- Permit/deny all other IP traffic in accordance with
!-- existing security policies and configurations.
!
```

```
class-map match-all drop-options-class
 match access-group name drop-affected-options
```

```
!
!
```

```
policy-map drop-opt-policy
 class drop-options-class
 drop
```

```
!
```

```
control-plane
 service-policy input drop-opt-policy
```

ACL support for filtering IP Options requires named ACLs. ACL support for filtering IP Options is not available in 12.0S or 12.2SX.

Additional information for filtering IP Options with access lists can be found at the following URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtipofil.html

Interface Access-lists: Internet edge routers that do not support CoPP or IP Options Selective drop can configure interface access-lists to drop packets that can be used to exploit this vulnerability.

Added access list entries should be implemented as part of existing network ingress traffic filters.

Transit Access-lists: The following ACL is specifically designed to block attack traffic and should be applied to all IPv4 interfaces of the device and should include topology-specific filters.

These ACL statements should be deployed at the network edge as part of a transit access-list which will protect the router where the ACL is configured as well as other devices behind it. Further information about transit ACLs is available in the white paper **Transit Access Control Lists: Filtering at Your Edge:**

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml

```
access-list 150 deny icmp any any echo
access-list 150 deny icmp any any information-request
access-list 150 deny icmp any any timestamp-request
access-list 150 deny icmp any any mask-request
access-list 150 deny tcp any any eq 465
access-list 150 deny 103 any any
access-list 150 deny 113 any any
```

```
!-- Permit/deny all other IP traffic in accordance with
!-- existing security policies and configurations.
```

```
interface serial 2/0
 ip access-group 150 in
```

Anti-Spoofing: This vulnerability can be exploited by a single, easily spoofed packet. Anti-spoof protection in the form of interface access-lists or unicast Reverse Path Forwarding can provide limited mitigation if properly configured. This mitigation should not be relied upon to provide 100% mitigation since spoofed packets may still enter the core from the interface expected by uRPF or allowed by anti-spoofing access-lists. Also care must be taken to ensure that the appropriate uRPF mode (loose or strict) is configured to ensure that legitimate packets are not dropped.

Additional information about unicast Reverse Path Forwarding is available at:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ft_urpf.html

Identification

IP Options Selective Drop: Once the command **ip options drop** is deployed, the command **show ip traffic** can be used to determine if packets with IP Options are being dropped by the router.

Example output for **show ip traffic**:

```
Edge-Router#show ip traffic
IP statistics:
  Rcvd: 181 total, 79 local destination
        0 format errors, 0 checksum errors, 0 bad hop count
```

```

    0 unknown protocol, 0 not a gateway
    0 security failures, 0 bad options, 0 with options
Opts: 0 end, 0 nop, 0 basic security, 0 loose source route
    0 timestamp, 0 extended security, 0 record route
    0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
    0 other
Frag: 0 reassembled, 0 timeouts, 0 couldn't reassemble
    0 fragmented, 0 couldn't fragment
Bcast: 0 received, 0 sent
Mcast: 0 received, 0 sent
Sent: 78 generated, 0 forwarded
Drop: 0 encapsulation failed, 0 unresolved, 0 no adjacency
    0 no route, 0 unicast RPF, 0 forced drop
    102 options denied
Drop: 0 packets with source IP address zero

```

ICMP statistics:

----- output truncated -----

In the above example the router has dropped 102 IP packets that had IP Options set.

Control Plane Policing: Once the CoPP configuration is deployed, the commands **show access-list drop-affected-options** and **show policy-map control-plane all** can be used to identify packets dropped by the CoPP policy. Additionally SNMP queries using the **Cisco QoS MIB CISCO-CLASS-BASED-QOS-MIB** can be used to track packets being dropped by CoPP. Packets being dropped by CoPP should be investigated to determine if they are attempts to exploit the vulnerability.

Example output for **show access-list drop-affected-options**:

```

Edge-Router#show access-list drop-affected-options
Extended IP access list drop-affected-options
 10 permit icmp any any echo option any-options (1569203 matches)
 20 permit icmp any any information-request option any-options
 30 permit icmp any any timestamp-request option any-options
 40 permit icmp any any mask-request option any-options
 50 permit pim any any option any-options
 60 permit tcp any any eq 465 option any-options
 70 permit tcp any any eq 465 option any-options

```

In the above example 1,569,203 ICMP echo packets that contained IP Options have been dropped by the access-list associated with CoPP.

Example output for **show policy-map control-plane all**:

```

Edge-Router#show policy-map control-plane all

Control Plane

Service-policy input: drop-opt-policy

Class-map: drop-options-class (match-all)
 1569203 packets, 109844210 bytes
 5 minute offered rate 1095000 bps, drop rate 1095000 bps
Match: access-group name drop-affected-options
drop

```

```
Class-map: class-default (match-any)
  113 packets, 12588 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match: any
```

In the above example class-map **drop-options-class** has dropped 1,569,203 packets.

Example output for an SNMP query using the **Cisco QoS MIB CISCO-CLASS-BASED-QOS-MIB**:

```
Linux# tinysnmpget 10.89.236.153 ha5d7ogu355 1.3.6.1.4.1.9.9.166.1.15.1.1.13

1.3.6.1.4.1.9.9.166.1.15.1.1.13.1043.1045 = Counter32 1569203
```

The output of this SNMP query matches the exceeded bytes that were dropped shown in the CLI output above for class-map: **drop-options-class**

1.3.6.1.4.1.9.9.166.1.15.1.1.13 is object **cbQosCMDropByte**.

1043.1045 is the table index number for a specific control-plane service policy class-map. The table index can be determined by SNMP walking OID: **1.3.6.1.4.1.9.9.166.1**. In this case **1043.1045** indicates class map **drop-options-class**.

Interface Access-lists: Once the interface access-list is deployed, the command `show access-list 150` can be used to identify packets it is dropping. Dropped packets should be investigated to determine if they are attempts to exploit the vulnerability.

Example output for **show access-list 150**:

```
Edge-Router#show access-list 150
Extended IP access list 150
 10 deny icmp any any echo (6154 matches)
 20 deny icmp any any information-request
 30 deny icmp any any timestamp-request (7667 matches)
 40 deny icmp any any mask-request
 50 deny tcp any any eq 465
 60 deny pim any any
 70 deny 113 any any
```

In the above example 6,154 ICMP echo packets and 7,667 ICMP timestamp-request packets that were either destined to the router or transiting through it have been dropped by the access-list configured on interface Serial 2/0.

NetFlow: Due to the way NetFlow interacts with process switched packets, NetFlow on most IOS platforms including all routers and Catalyst 6500 switches will not report flows for any packets containing IP Options. The exception to this is the Catalyst 4500 switch which will report these flows. Additional information for configuring NetFlow on Catalyst 4500 switches is available at:

Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(20)EW - Configuring NetFlow Statistics Collection

<http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/20ew/configuration/guide/nfswitch>

NetFlow can be configured on Catalyst 4500 series switches to determine if attempts are in progress

to exploit this vulnerability.

```
Cat4506#show ip cache flow
```

```
IP Flow Switching Cache, 17826816 bytes
 7 active, 262137 inactive, 16485 added
19196 aged polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
```

```
IP Sub Flow Cache, 1081480 bytes
 7 active, 65529 inactive, 58 added, 58 added to flow
 0 alloc failures, 0 force free
 1 chunk, 1 chunk added
last clearing of statistics never
```

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idl
TCP-Telnet	9	0.0	22	41	0.0	9.5	
TCP-other	1	0.0	12	68	0.0	35.3	
UDP-NTP	14	0.0	1	76	0.0	0.0	
ICMP	4	0.0	25	63	0.0	21.0	
IP-other	4	0.0	7	72	0.0	23.0	
Total:	32	0.0	11	52	0.0	9.3	

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP
Vl100	10.89.236.135	Gi2/25	192.168.3.2	01	0000
Vl146	192.168.146.3	Null	224.0.0.10	58	0000

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP
Vl146	192.168.146.3	Null	224.0.0.5	59	0000
Vl146	10.89.1.182	Local	192.168.128.4	06	0950
Vl100	10.89.236.135	Gi2/25	192.168.3.2	67	0000
Vl100	10.89.236.135	Gi2/25	192.168.3.2	71	0000
Vl100	10.89.236.135	Gi2/25	192.168.3.2	06	0506

In the above example from the Catalyst 4500 switch, there are several ICMP (Pr = 01), PIM (Pr = 67), PGM (Pr = 71), and TCP/465 (DstP = 01D1) flows. Each of these flows may be an attempt to exploit the vulnerability described within this document and should be compared to the baseline utilization of traffic using these protocols and ports on the production network.

To only view ICMP (Hex 01), PIM (Hex 67), PGM (Hex 71), and TCP/465 (Hex 01D1) flows, the command **show ip cache flow | include SrcIf|01|67|71|01D1** may be used as shown here:

```
Cat4506#show ip cache flow | include SrcIf|01|67|71|01D1
SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr  SrcP  DstP
Vl100     10.89.236.135    Gi2/25     192.168.3.2      01 0000 0083
Vl100     10.89.236.135    Gi2/25     192.168.3.2      67 0000 0000
Vl100     10.89.236.135    Gi2/25     192.168.3.2      71 0000 0000
Vl100     10.89.236.135    Gi2/25     192.168.3.2      06 0506 01D1
```

Cisco PIX/ASA/FWSM Firewalls



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.

Mitigation

The Cisco PIX Security Appliance, Cisco ASA Adaptive Security Appliance, and Firewall Service Modules (FWSM) for Cisco Catalyst 6500 Switches and Cisco 7600 Routers will, by default, drop all packets containing IP options they receive on any interface. No configuration changes are required to enable this functionality.

Identification

After the firewall drops a packet with IP options, it will generate an informational level (severity 6) *syslog* message. The severity level of the *syslog* message can be adjusted if logging all informational messages creates too great a performance load on the firewall or provides too much detail. The *syslog* message is [106012](#), which has this format:

106012: Deny IP from <Source IP Address> to <Destination IP Address>, IP options: "<Specific Option set in packet>"

Due to the nature of this vulnerability, any ICMP type 8, type 13, type 15, type 17 packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet carrying an IP option could potentially be crafted to exploit the issue. All *syslog* 106012 messages should be investigated as potential indications of attempts to exploit this vulnerability.

Additionally, if the edge router is configured with **IP options drop**, any *syslog* 106012 messages are the result of packets generated on the internal network or from a device on the DMZ network segment inside the edge router. These packets should be fully investigated to determine the true source.

Cisco IOS XR Router



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.

Mitigation

Interface Access Lists: The following access list is specifically designed to block attack traffic and should be applied to all IPv4 interfaces of the device and should include topology-specific filters. The access list denies potential exploit traffic from all source IP addresses to the network infrastructure address block (192.0.2.0/24).

```
ipv4 access-list ios-xr-infrastructure-acl
 10 deny icmp any 192.0.2.0 0.0.0.255 echo
 20 deny icmp any 192.0.2.0 0.0.0.255 information-request
 30 deny icmp any 192.0.2.0 0.0.0.255 timestamp-request
 40 deny icmp any 192.0.2.0 0.0.0.255 mask-request
 50 deny tcp any 192.0.2.0 0.0.0.255 eq 465
 60 deny 103 any 192.0.2.0 0.0.0.255
 70 deny 113 any 192.0.2.0 0.0.0.255

!-- Permit/deny all other IP traffic in accordance with
!-- existing security policies and configurations.
```

```
interface POS 0/2/0/2
  ipv4 access-group ios-xr-infrastructure-acl ingress
```

The white paper entitled **Protecting Your Core: Infrastructure Protection Access Control Lists** presents guidelines and recommended deployment techniques for infrastructure protection access lists:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml.

Information about configuring access lists on Cisco IOS-XR is available

at:http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.2/addr_serv/command/reference/ir32acl.htm

Identification

After the interface access list is deployed, the command **show access-list ipv4 ios-xr-infrastructure-acl** can be used to identify the number of packets being dropped. Dropped packets should be investigated to determine if they are attempts to exploit the issue.

Example output for **show access-list ipv4 ios-xr-infrastructure-acl**:

```
RP/0/RP0/CPU0:CRS-A_IOX#show access-lists ios-xr-infrastructure-acl
ipv4 access-list ios-xr-infrastructure-acl
10 deny icmp any 192.0.2.0 0.0.0.255 echo
20 deny icmp any 192.0.2.0 0.0.0.255 information-request
30 deny icmp any 192.0.2.0 0.0.0.255 timestamp-request
40 deny icmp any 192.0.2.0 0.0.0.255 mask-request
50 deny tcp any 192.0.2.0 0.0.0.255 eq 465
60 deny 103 any 192.0.2.0 0.0.0.255 (49 matches)
70 deny 113 any 192.0.2.0 0.0.0.255 (711 matches)
```

In the example above, 49 PIM packets and 711 PGM packets have been dropped by the **access-list ipv4 ios-xr-infrastructure-acl**.

Cisco Intrusion Prevention System (IPS)

Identification

Beginning with signature update S267, IPS signatures 5832.0 - 5832.3 trigger a High severity alarm on potential attempts to exploit the Crafted IP Options Vulnerability which may indicate a Denial of Service or arbitrary code execution attack. The following high severity events were triggered by signatures 5830.0, 5830.1, 5830.2, and 5830.3 after a potential attempt to exploit the Crafted IP Options Vulnerability on the target victim at IP address 192.168.0.10:

Signature: 5830.0 showing a Crafted ICMP packet

```
evIdsAlert: eventId=1166726998236416961 vendor=Cisco severity=high
originator:
  hostId: R4-IPS4240a
  appName: sensorApp
  appInstanceId: 9634
time: January 25, 2007 2:56:45 AM UTC offset=-360 timeZone=CST
signature: description=IOS Crafted IP Option Vulnerability id=5832 ver
  subSigId: 0
sigDetails: Crafted ICMP packet
marsCategory: DoS/Network/ICMP
marsCategory: DoS/NetworkDevice
marsCategory: Info/UncommonTraffic/ICMP
marsCategory: Info/UncommonTraffic/Suspicious
```

marsCategory: Penetrate/BufferOverflow/Misc
marsCategory: Penetrate/ProtocolAnomaly/Misc
interfaceGroup: vs0
vlan: 0
participants:
 attacker:
 addr: 192.0.2.100 locality=OUT
 target:
 addr: 192.168.0.10 locality=OUT
 os: idSource=unknown type=unknown relevance=unknown
riskRatingValue: 85 targetValueRating=medium
threatRatingValue: 85
interface: ge0_0
protocol: icmp

Signature: 5830.1 showing a Crafted PIMv2 packet

evIdsAlert: eventId=1166726998236417102 vendor=Cisco **severity=high**
originator:
 hostId: R4-IPS4240a
 appName: sensorApp
 appInstanceId: 9634
time: January 25, 2007 3:00:01 AM UTC offset=-360 timeZone=CST
signature: description=IOS Crafted IP Option Vulnerability **id=5832 ver**
 subsigId: 1
 sigDetails: **Crafted PIMv2 Packet**
 marsCategory: DoS/Network/Misc
 marsCategory: DoS/NetworkDevice
 marsCategory: Info/UncommonTraffic/Suspicious
 marsCategory: Penetrate/BufferOverflow/Misc
 marsCategory: Penetrate/ProtocolAnomaly/Misc
interfaceGroup: vs0
vlan: 0
participants:
 attacker:
 addr: 192.0.2.100 locality=OUT
 target:
 addr: 192.168.0.10 locality=OUT
 os: idSource=unknown type=unknown relevance=unknown
riskRatingValue: 85 targetValueRating=medium
threatRatingValue: 85
interface: ge0_0
protocol: IP protocol 103

Signature: 5830.2 showing a Crafted PGM packet

evIdsAlert: eventId=1166726998236417251 vendor=Cisco **severity=high**
originator:
 hostId: R4-IPS4240a
 appName: sensorApp
 appInstanceId: 9634
time: January 25, 2007 3:03:33 AM UTC offset=-360 timeZone=CST
signature: description=IOS Crafted IP Option Vulnerability **id=5832 ver**
 subsigId: 2
 sigDetails: **Crafted PGM packet**
 marsCategory: DoS/Network/Misc
 marsCategory: DoS/NetworkDevice
 marsCategory: Info/UncommonTraffic/Suspicious
 marsCategory: Penetrate/BufferOverflow/Misc
 marsCategory: Penetrate/ProtocolAnomaly/Misc
interfaceGroup: vs0
vlan: 0

```
participants:
  attacker:
    addr: 192.0.2.100  locality=OUT
  target:
    addr: 192.168.0.10  locality=OUT
    os:  idSource=unknown  type=unknown  relevance=unknown
riskRatingValue: 85  targetValueRating=medium
threatRatingValue: 85
interface: ge0_0
protocol: IP protocol 113
```

Signature: 5830.3 showing a Crafted URD packet

```
evIdsAlert: eventId=1166726998236417143  vendor=Cisco  severity=high
originator:
  hostId: R4-IPS4240a
  appName: sensorApp
  appInstanceId: 9634
time: January 25, 2007 3:01:00 AM UTC  offset=-360  timeZone=CST
signature:  description=IOS Crafted IP Option Vulnerability  id=5832  ver
  subsigId: 3
  sigDetails: Crafted URD packet
  marsCategory: DoS/Network/TCP
  marsCategory: DoS/NetworkDevice
  marsCategory: Info/UncommonTraffic/Suspicious
  marsCategory: Info/UncommonTraffic/TCPIPOptions
  marsCategory: Penetrate/BufferOverflow/Misc
  marsCategory: Penetrate/ProtocolAnomaly/TCPIP
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: 192.0.2.100  locality=OUT
    port: 1286
  target:
    addr: 192.168.0.10  locality=OUT
    port: 465
    os:  idSource=unknown  type=unknown  relevance=unknown
riskRatingValue: 85  targetValueRating=medium
threatRatingValue: 85
interface: ge0_0
protocol: tcp
```

Cisco Security MARS (CS MARS)

Identification

Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) can display Cisco firewall syslog messages pertaining to IP options.

Figure 1 depicts a sample query (which can be converted to both a rule and a report) searching for PIX/ASA/FWSM Syslog Message 106012 generated within the past 24 hours.

Figure 1. Cisco Security MARS Sample Query for Syslog Message 106012

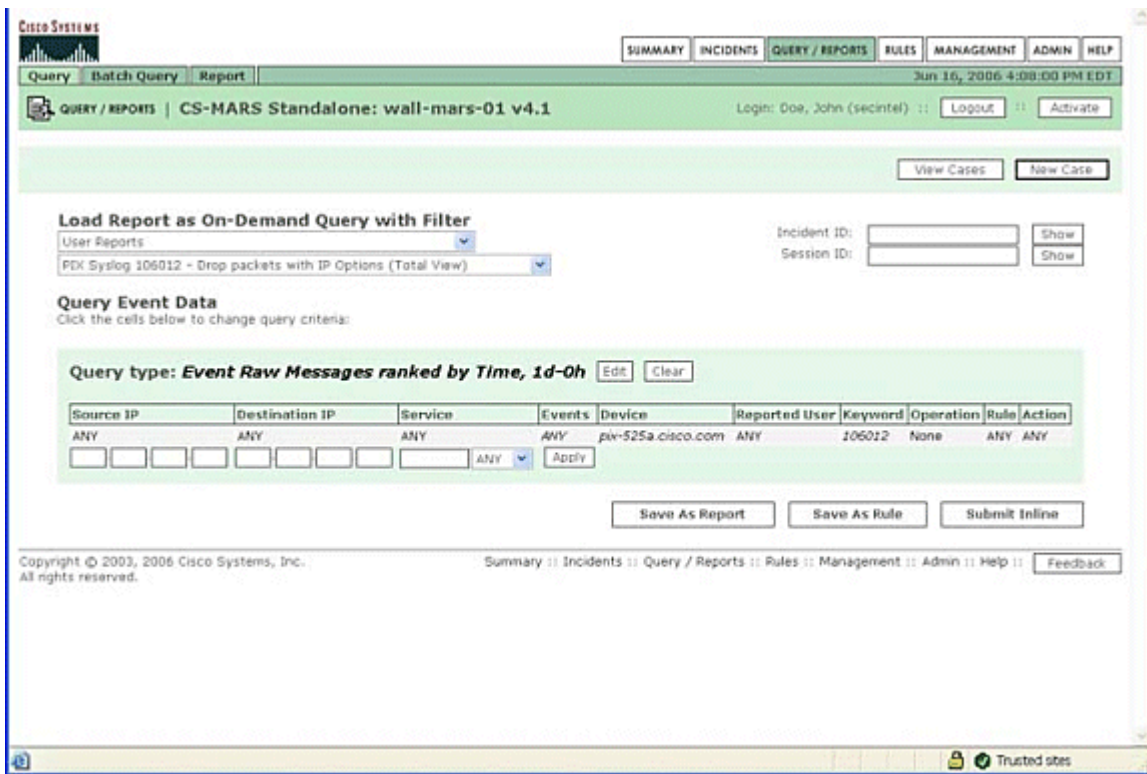


Figure 2 shows the messages that Cisco Security MARS will display when queried for syslog messages from firewalls pertaining to the IP options syslog message (with a query time frame of the past six hours).

Figure 2. Cisco Security MARS Sample Output for Syslog Message 106012 Query

Query Event Data
Click the cells below to change query criteria:

Query type: **Event Raw Messages ranked by Time, 0d-6h:00m**

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	pix-525a.cisco.com	ANY	106012	None	ANY	ANY

Query Results

Event / Session / Incident ID	Event Type	Time	Reporting Device	Raw Message	Path / Mitigation	Tune
E:368737655, S:368737655	Unknown Device Event Type	Jun 16, 2006 2:42:51 PM EDT	pix-525a.cisco.com	<166>%PIX-6-: Deny IP from 10.89.236.147 to 10.89.236.131, IP options: "Strict Src Routing"	N/A	False Positive
E:368737657, S:368737657	Unknown Device Event Type	Jun 16, 2006 2:42:51 PM EDT	pix-525a.cisco.com	<166>%PIX-6-: Deny IP from 10.89.236.147 to 10.89.236.131, IP options: "Strict Src Routing"	N/A	False Positive
E:368737653, S:368737653	Unknown Device Event Type	Jun 16, 2006 2:42:50 PM EDT	pix-525a.cisco.com	<166>%PIX-6-: Deny IP from 10.89.236.147 to 10.89.236.131, IP options: "Strict Src Routing"	N/A	False Positive
E:368737651, S:368737651	Unknown Device Event Type	Jun 16, 2006 2:42:43 PM EDT	pix-525a.cisco.com	<166>%PIX-6-: Deny IP from 10.89.236.147 to 10.89.236.131, IP options: "Loose Src Routing"	N/A	False Positive
E:368737649, S:368737649	Unknown Device Event Type	Jun 16, 2006 2:42:42 PM EDT	pix-525a.cisco.com	<166>%PIX-6-: Deny IP from 10.89.236.147 to 10.89.236.131, IP options: "Loose Src Routing"	N/A	False Positive
E:368737647, S:368737647	Unknown Device Event Type	Jun 16, 2006 2:42:41 PM EDT	pix-525a.cisco.com	<166>%PIX-6-: Deny IP from 10.89.236.147 to 10.89.236.131, IP options: "Loose Src Routing"	N/A	False Positive

1 to 6 of 6 25 per page

Figure 3 depicts the previous query converted to a rule that will execute when the Cisco PIX security appliance generates syslog messages indicating that packets with IP options have been dropped.

Figure 3. Cisco Security MARS Sample Rule for Syslog Message 106012 Query

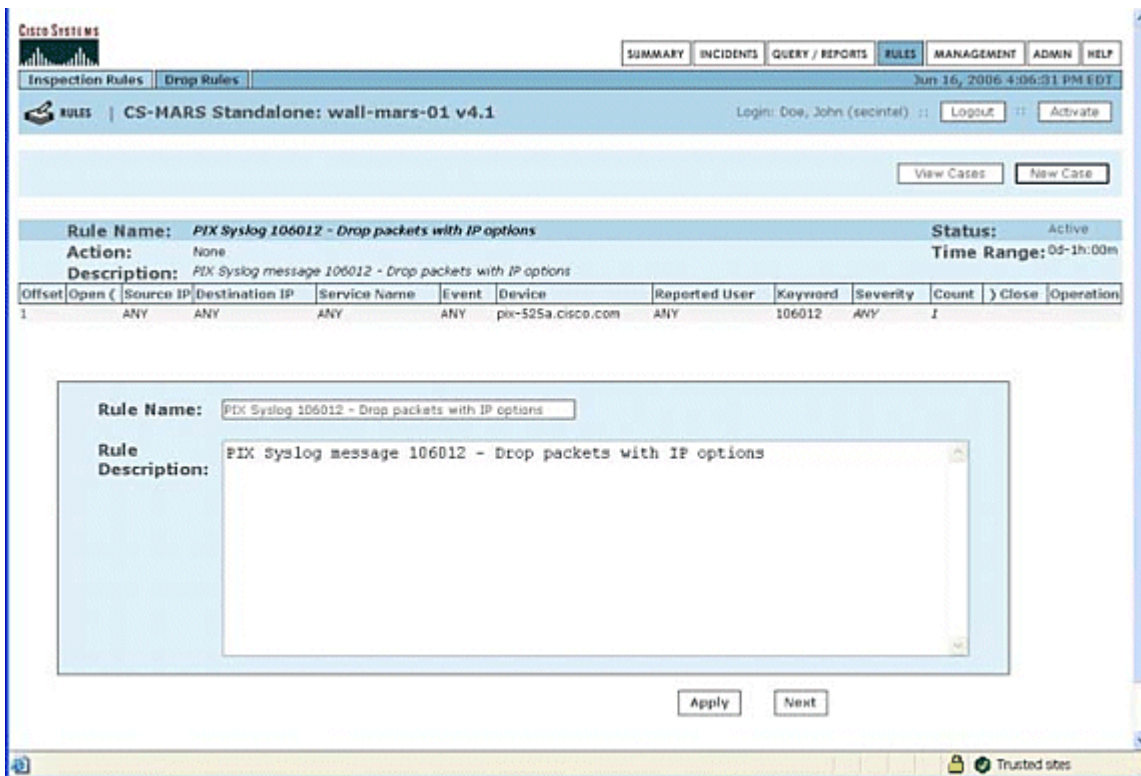
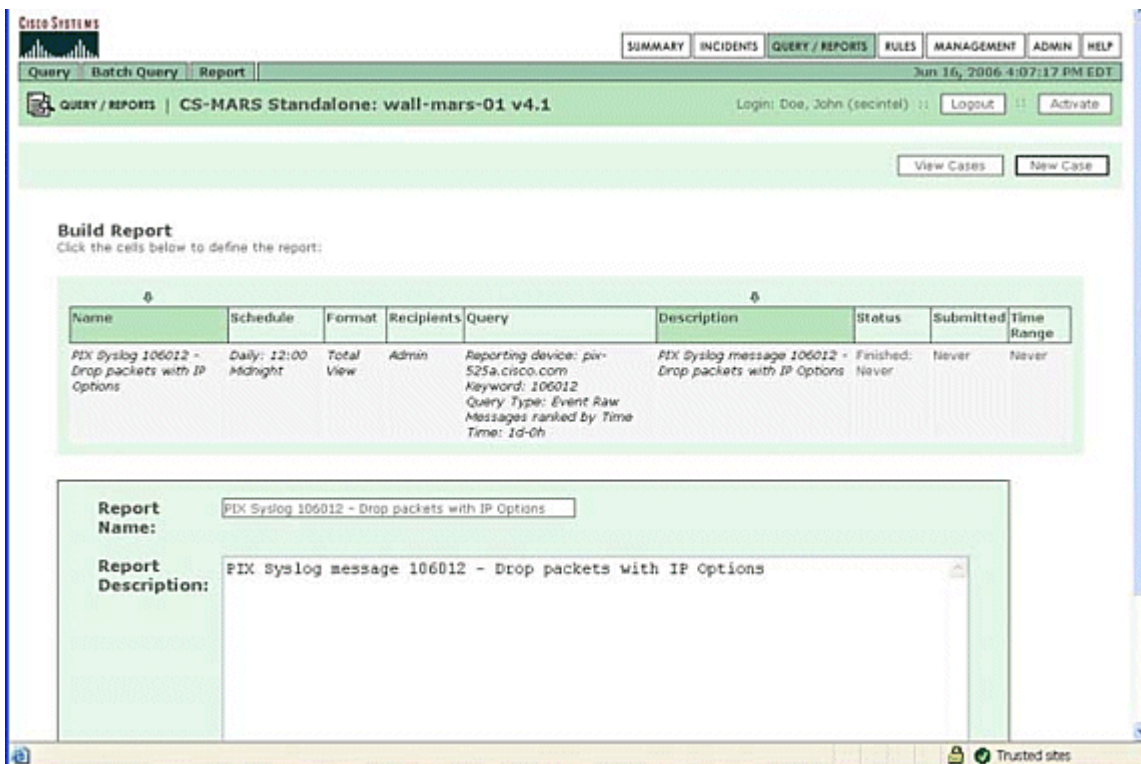


Figure 4 depicts the recurring report pertaining to instances when the IP options rule has triggered. This report, as currently configured, will be sent to the Admin user at midnight on a daily basis.

Figure 4. Cisco Security MARS Sample Report for Syslog Message 106012 Query



CS MARS can display Cisco IPS messages pertaining to the Crafted IP Options vulnerability. Figure 5 depicts a sample query (which can be converted to both a rule and a report) searching for events triggered by Cisco IPS signature 5832 within the past 4 hours.

Figure 5. Cisco Security MARS Sample Query for Cisco IPS signature 5832

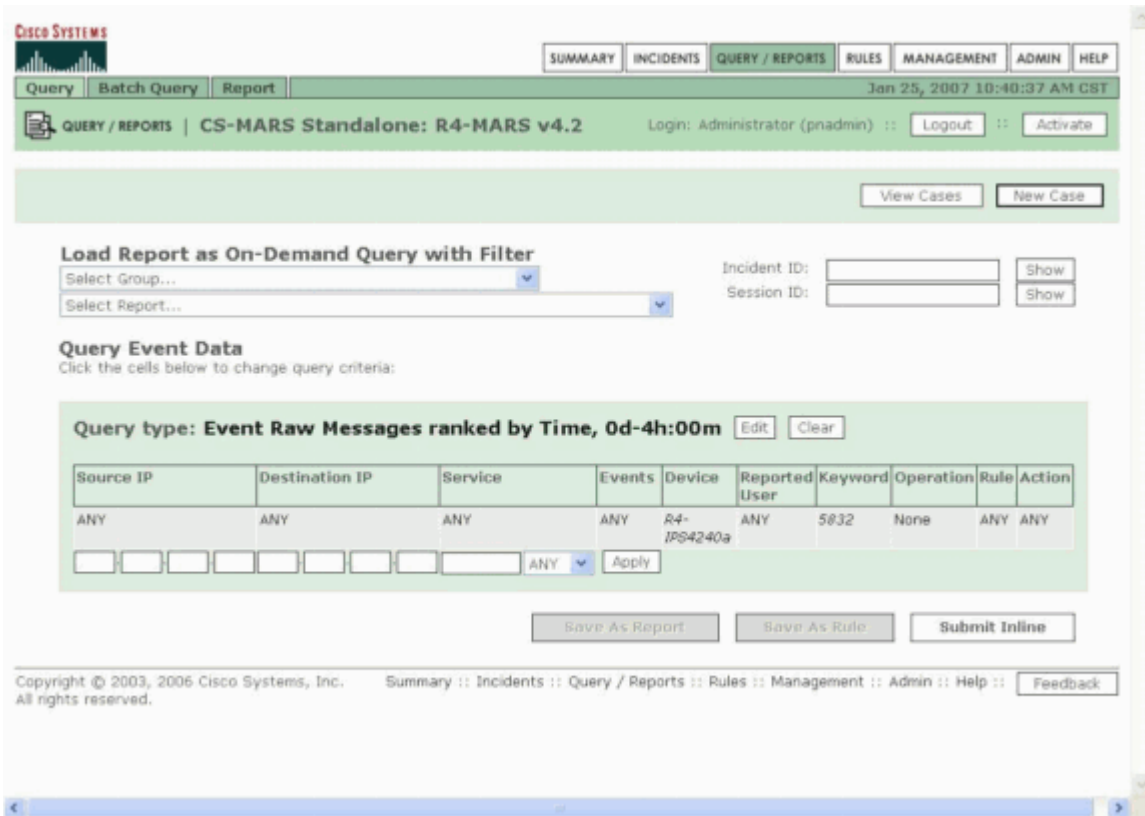
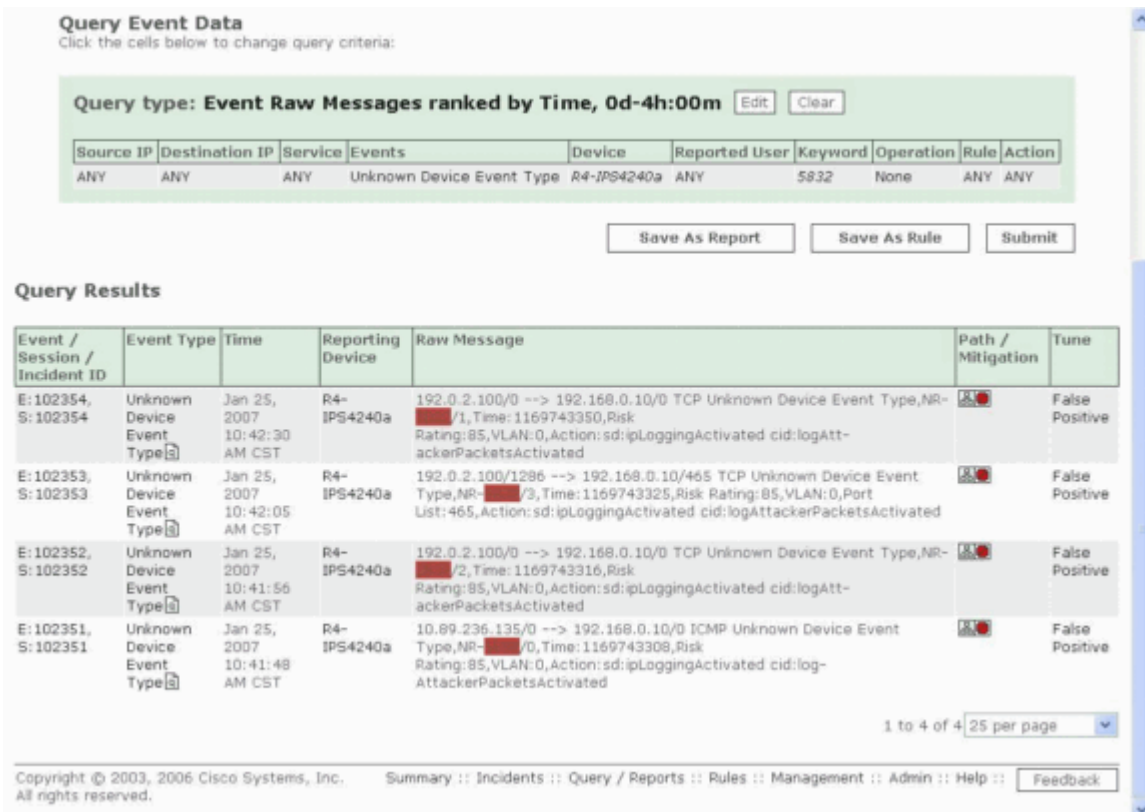


Figure 6 shows the messages that Cisco Security MARS will display when queried for events triggered by Cisco IPS signature 5832 (with a query time frame of the past four hours).

Figure 6. Cisco Security MARS Sample Output for Cisco IPS signature 5832 Query



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 1.1	2007- January- 25	Added the Cisco Intrusion Prevention System (IPS) section, and added information and graphics to the Cisco Security MARS (CS MARS) section.
Revision 1.0	2007- January- 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. 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

- [RFC 791 - INTERNET PROTOCOL](#) 
- [GSR: Receive Access Control Lists](#)
- [Transit Access Control Lists: Filtering at Your Edge](#)
- [Protecting Your Core: Infrastructure Protection Access Control Lists](#)
- [IP Options Selective Drop](#)
- [Control Plane Policing](#)
- [Deploying Control Plane Policing](#)
- [Cisco Network Foundation Protection \(NFP\) White Papers](#)
- [ACL Support for Filtering IP Options](#)
- [Unicast Reverse Path Forwarding Loose Mode](#)
- [Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2\(20\)EW - Configuring NetFlow Statistics Collection](#)

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](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)