

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Vulnerabilities in Cisco Video Surveillance Products

<http://www.cisco.com/warp/public/707/cisco-amb-20090624-video.shtml>

Revision 1.1

Last Updated 2009 June 25 1800 UTC (GMT)

For Public Release 2009 June 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 *Vulnerabilities in Cisco Video Surveillance Products* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

There are multiple vulnerabilities in the Cisco Video Surveillance Stream Manager for Services Platforms and Integrated Services Platforms. The following subsections summarize these vulnerabilities:

Denial of service (DoS) 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 reboot. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through a packet using UDP port 37000. An attacker could exploit this vulnerability using spoofed packets.

This vulnerability has been assigned CVE identifier CVE-2009-2045.

Information disclosure vulnerability: This vulnerability can be exploited remotely with authentication and without end-user interaction. Successful exploitation of this vulnerability may allow information disclosure to allow an attacker to learn information about the affected device.

The attack vectors for exploitation are through packets using the following protocols and ports:

- HTTP using TCP port 80.
- HTTPS using TCP port 443.

This vulnerability has been assigned CVE identifier CVE-2009-2046.

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-20090624-video.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.

All the countermeasures in this document apply to the *denial of service* vulnerability. NetFlow records can be used to aid in the identification of traffic flows that may be attempts to exploit both the *information disclosure* vulnerability and the *denial of service* vulnerability.

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

- Infrastructure access control lists (iACLs)
- 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 *denial of service* vulnerability.

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.

Because the potential exists that a trusted networking client could become affected by a worm that does not use packets with spoofed source addresses, Unicast RPF and IPSG do not provide complete protection against these vulnerabilities.

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)
- Unicast Reverse Path Forwarding (Unicast RPF)

These protection mechanisms filter and drop, as well as verify the source IP address of, packets that are attempting to exploit the *denial of service* vulnerability.

Cisco IOS NetFlow flow records can provide visibility into network-based exploitation attempts. This is the only countermeasure applicable to the *information disclosure* vulnerability.

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 these vulnerabilities.

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can also provide visibility through incidents, 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 depends 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

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 these vulnerabilities when the attack originates from a trusted source address.

The iACL policy denies unauthorized packets on UDP port 37000 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 the host at 192.168.100.1 is considered a trusted source that requires access to the affected devices. 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.

Additional information about iACLs is 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 port
!

permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 37000

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

deny udp any 192.168.60.0 0.0.0.255 eq 37000

!
!-- 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
!
!-- 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 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 *denial of service* vulnerability described in this document can be exploited by spoofed IP packets. The proper deployment and configuration of Unicast Reverse Path Forwarding (Unicast RPF) can provide protection mechanisms for spoofing related to the *denial of service* vulnerability.

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 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. The proper deployment and configuration of IPSG coupled with strict mode Unicast RPF can provide the most effective means of spoofing protection to help mitigate the *denial of service* vulnerability.

Additional information about the deployment and configuration of IPSG is 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 packets on UDP port 37000 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 udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 37000
 20 deny udp any 192.168.60.0 0.0.0.255 eq 37000( 116 matches )
 30 deny ip any 192.168.60.0 0.0.0.255
router#
```

In the preceding example, access list *Infrastructure-ACL-Policy* has dropped **116 packets on UDP port 37000** for access control list entry (ACE) line 20.

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 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=18, 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	128	
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
      128 no route, 128 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
```

router#

In the preceding **show cef drop** and **show ip traffic** examples, Unicast RPF has dropped **128 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 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 these vulnerabilities. Administrators are advised to investigate flows to determine whether they are attempts to exploit these vulnerabilities or whether they are legitimate traffic flows.

router# **show ip cache flow**

IP packet size distribution (7559320 total packets):

1-32	64	96	128	160	192	224	256	288	320	352	384	416	448	480
.000	.282	.425	.075	.016	.022	.007	.002	.005	.004	.002	.006	.002	.000	.001
512	544	576	1024	1536	2048	2560	3072	3584	4096	4608				
.001	.000	.007	.016	.118	.000	.000	.000	.000	.000	.000				

IP Flow Switching Cache, 4456704 bytes

67 active, 65469 inactive, 952199 added

85186208 ager polls, 0 flow alloc failures

Active flows timeout in 2 minutes

Inactive flows timeout in 60 seconds

IP Sub Flow Cache, 533256 bytes

67 active, 16317 inactive, 952199 added, 952199 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	37	0.0	16	40	0.0	2.6
46.1						
TCP-FTP	2869	0.0	1	54	0.0	0.5
43.9						
TCP-FTPD	231	0.0	3	45	0.0	
0.1	5.3					
TCP-WWW	21964	0.0	14	623	0.2	14.7
39.1						
TCP-SMTP	725	0.0	30	1022	0.0	54.8
57.5						

TCP-other	68428	0.0	34	491	2.1	28.5
18.6						
UDP-DNS	59620	0.0	2	64	0.1	7.5
57.0						
UDP-NTP	28231	0.0	1	76	0.0	0.4
60.5						
UDP-other	415569	0.3	7	85	2.7	9.9
57.0						
ICMP	242737	0.2	3	161	0.7	26.9
50.7						
IGMP	36627	0.0	2	40	0.0	57.5
43.0						
IPINIP	8632	0.0	8	64	0.0	110.1
10.4						
IPv6INIP	8630	0.0	8	104	0.0	110.4
10.0						
IP-other	57834	0.0	10	93	0.5	91.5
16.2						
Total:	952134	0.8	7	245	6.7	23.9
48.4						

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP
DstP Pkts					
Gi0/0	192.168.208.127	Nu0	192.168.60.4	11	0495
9088					4
Gi0/0	192.168.208.127	Gi0/1	192.168.60.4	11	0429
9088					8
Gi0/0	192.168.208.127	Nu0	192.168.60.21	11	05BB
9088					8
Gi0/0	192.168.208.127	Local	192.168.60.20	11	06F1
9088					3
Gi0/0	192.168.208.76	Gi0/1	192.168.60.66	11	9EA7
00A1					3
Gi0/0	192.168.208.76	Nu0	192.168.128.22	11	9EA3
00A1					3
Gi0/0	192.168.208.76	Nu0	192.168.128.22	11	9EA4
00A1					3
Gi0/0	192.168.208.76	Nu0	192.168.128.22	11	9EA5
00A1					3
Gi0/0	192.168.208.76	Nu0	192.168.128.23	11	9EA6
00A1					3
Gi0/0	192.168.10.201	Gi0/1	192.168.60.102	06	0984
01BB					62
Gi0/0	192.168.31.68	Gi0/1	192.168.60.138	06	0911
0050					43

router#

In the preceding example, there are multiple flows for **UDP** port **37000** (hex value **9088**), for **HTTPS** packets on **TCP** port **443** (hex value **01BB**), and **HTTP** packets on **TCP** port **80** (hex value **0050**).

This traffic is sent to addresses within the 192.168.60.0/24 address block, which is used for infrastructure devices. The packets in these flows may be spoofed and may indicate an attempt to exploit these vulnerabilities. Administrators are advised to compare these flows to baseline utilization for packets sent on UDP port 37000 (Hex value 9088), HTTP packets sent on TCP port 80 (Hex value 0050), and HTTPS packets sent on TCP port 443 (Hex value 01BB) and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

To view only the traffic flows for packets on UDP port 37000 (hex value 9088), the command **show ip cache flow | include SrcIf_11.*9088** will display the related UDP NetFlow records as shown here:

UDP Flows

```
router# show ip cache flow | include SrcIf|_11_.*9088
SrcIf          SrcIPAddress      DstIf          DstIPAddress      Pr SrcP
DstP  Pkts
Gi0/0          192.168.208.127  Gi0/1          192.168.60.3      11 044B
9088           4
Gi0/0          192.168.208.127  Nu0            192.168.60.4      11 0429
9088           6
Gi0/0          192.168.208.127  Gi0/1          192.168.60.2      11 0878
9088           4
router#
```

To view only the traffic flows for packets on HTTP packets on TCP port 80 (Hex value 0050) and HTTPS packets on TCP port 443 (hex value 01BB), the command **show ip cache flow | include SrcIf_06.*(0050|01BB)_** will display the related TCP NetFlow records as shown here:

TCP Flows

```
router# show ip cache flow | include SrcIf|_06_.*(0050|01BB)
SrcIf          SrcIPAddress      DstIf          DstIPAddress      Pr SrcP
DstP  Pkts
Gi0/0          192.168.10.201   Gi0/1          192.168.60.102   06 0984
01BB           62
Gi0/0          192.168.31.68    Gi0/1          192.168.60.138   06 0911
0050           43
router#
```

Cisco ASA, PIX, and FWSM Firewalls

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 these vulnerabilities when the attack originates from a trusted source address.

The tACL policy denies unauthorized packets on UDP port 37000 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 the host at 192.168.100.1 is considered a trusted source that requires access to the 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 in [Transit Access Control Lists: Filtering at Your Edge](#).

```
!  
!-- Include any explicit permit statements for trusted sources  
!-- that require access on the vulnerable ports  
!  
  
access-list tACL-Policy extended permit udp host 192.168.100.1  
192.168.60.0 255.255.255.0 eq 37000  
  
!  
!-- The following vulnerability-specific access control entry  
!-- (ACE) can aid in identification of attacks  
!  
  
access-list tACL-Policy extended deny udp any 192.168.60.0  
255.255.255.0 eq 37000  
  
!  
!-- 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

One vulnerability that is described in this document can be exploited by spoofed IP packets. The proper deployment and configuration of Unicast RPF can provide protection mechanisms for spoofing related to the *denial of service* vulnerability.

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 packets on UDP port 37000 that have been filtered. Administrators are advised to investigate filtered packets to determine whether they are attempts to exploit this vulnerability. Example output for **show access-list tACL-Policy** follows:

```
firewall# show access-list tACL-Policy
access-list tACL-Policy; 3 elements
access-list tACL-Policy line 1 extended permit udp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 37000 (hitcnt=0)
access-list tACL-Policy line 2 extended deny udp any 192.168.60.0
255.255.255.0 eq 37000 ( hitcnt=232)
access-list tACL-Policy line 3 extended deny ip any any (hitcnt=8)
firewall#
```

In the preceding example, access list *tACL-Policy* has dropped **232 packets on UDP port 37000** 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 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 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 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 in [Creating a Regular Expression](#).

```
firewall# show logging | grep 106023
Feb 21 2009 02:15:13: %ASA-4-106023: Deny udp src
outside:192.0.2.18/26944
dst inside:192.168.60.191/37000 by access-group "ACL-Policy"
Feb 21 2009 02:15:13: %ASA-4-106023: Deny udp src
outside:192.2.0.200/26945
dst inside:192.168.60.33/37000 by access-group "tACL-Policy"
```

```
firewall#
```

In the preceding example, the messages logged for the tACL *tACL-Policy* show potentially spoofed packets for **UDP port 37000** sent to the address block assigned to the infrastructure devices.

Additional information about syslog messages for ASA and PIX security appliances is in [Cisco Security Appliance System Log Messages](#). Additional information about syslog messages for the FWSM is 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 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 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 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 these 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 in [Creating a Regular Expression](#).

```
firewall# show logging | grep 106021
Jun 10 2009 02:15:13: %ASA-1-106021: Deny UDP reverse path check from
192.168.60.1 to 192.168.60.100 on interface outside
Jun 10 2009 02:15:13: %ASA-1-106021: Deny UDP reverse path check from
192.168.60.2 to 192.168.60.100 on interface outside
```

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          19
firewall#
```

In the preceding example, Unicast RPF has dropped **19 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

Cisco Intrusion Prevention System

Administrators can use Cisco Intrusion Prevention System (IPS) appliances and services modules to provide threat detection and help prevent attempts to exploit the vulnerabilities that are described in this document. These vulnerabilities may be detected by the following signatures:

- 16755/0 - Cisco Video Surveillance Stream Manager for Services Platforms and Integrated Services Platforms DoS
- 16733/0 - Cisco IP Camera Info Disclosure
- 16733/1 - Cisco IP Camera Info Disclosure

16755/0 - Cisco Video Surveillance Stream Manager for Services Platforms and Integrated Services Platforms DoS

Beginning with signature update S409 for sensors running Cisco IPS version 6.x or 5.x, one of these vulnerabilities can be detected by signature 16755/0 (Signature Name: Cisco Video Surveillance Stream Manager for Services Platforms and Integrated Services Platforms DoS). Signature 16755/0 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 16755/0 fires when a single crafted packet sent using UDP port 37000 that attempts a DoS attempt against Cisco Video Surveillance Stream Manager for Services Platforms and Integrated Services Platforms. Firing of this signature may indicate a potential exploit of these vulnerabilities.

16733/0 - Cisco IP Camera Info Disclosure

Beginning with signature update S409 for sensors running Cisco IPS version 6.x or 5.x, one of these vulnerabilities can be detected by signature 16733/0 (Signature Name: Cisco IP Camera Info Disclosure). Signature 16733/0 is enabled by default, triggers a *Medium* severity event, has a signature fidelity rating (SFR) of 95, and is configured with a default event action of **produce-alert**.

Signature 16733/0 fires when a single IP flow that attempts to exploit an information disclosure vulnerability in Cisco Video Surveillance 2500 IP Cameras is detected. Firing of this signature may indicate a potential exploit of these vulnerabilities.

16733/1 - Cisco IP Camera Info Disclosure

Beginning with signature update S409 for sensors running Cisco IPS version 6.x or 5.x, one of these vulnerabilities can be detected by signature 16733/1 (Signature Name: Cisco IP Camera Info Disclosure). Signature 16733/1 is enabled by default, triggers a *Medium* severity event, has a signature fidelity rating (SFR) of 95, and is configured with a default event action of **produce-alert**.

Signature 16733/1 fires when a single IP flow that attempts to exploit an information disclosure vulnerability in Cisco Video Surveillance 2500 IP Cameras is detected. Firing of this signature may indicate a potential exploit of these vulnerabilities.

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 vulnerabilities that are 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 that are deployed in inline protection mode provides threat prevention against an attack that is attempting to exploit the vulnerabilities that are 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: 16755/0 - Cisco Video Surveillance Stream Manager for Services Platforms and Integrated Services Platforms DoS

```
IPS# show events alert
evIdsAlert: eventId=1238718211601194046 severity=medium vendor=Cisco
originator:
  hostId: IPS
  appName: sensorApp
  appInstanceId: 424
time: 2009/06/24 21:31:23 2009/06/24 16:31:23 CDT
signature: description=Cisco Video Surveillance Stream Manager for
Services Platforms and Integrated Services Platforms DoS id=16755
created=20090624 type=vulnerability version=S409
  subsigId: 0
  sigDetails: Cisco Video Surveillance Stream Manager for Services
Platforms and Integrated Services Platforms DoS
  marsCategory: DoS/MiscServer
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=OUT 192.168.150.129
    port: 37000
  target:
    addr: locality=OUT 192.168.60.128
    port: 37000
os: idSource=unknown relevance=relevant type=unknown
```

triggerPacket:

-- *CLI Output Truncated* --

riskRatingValue: attackRelevanceRating=relevant
targetValueRating=medium 67
threatRatingValue: 67
interface: ge0_0
protocol: udp

Signature: 16733/0 - Cisco IP Camera Info Disclosure

IPS# **show events alert**

evIdsAlert: eventId=1238718211601194128 severity=medium vendor=Cisco
originator:
 hostId: R3-A041-IPS4240
 appName: sensorApp
 appInstanceId: 424
time: 2009/06/24 21:59:00 2009/06/24 16:59:00 CDT
signature: description=Cisco IP Camera Info Disclosure id=16733
created=20090624 type=vulnerability version=S409
 subsigId: 0
 sigDetails: Remote file access
 marsCategory: Penetrate/ViewFiles/Sensitive
interfaceGroup: vs0
vlan: 0
participants:
 attacker:
 addr: locality=OUT 192.168.208.63
 port: 32782
 target:
 addr: locality=OUT 192.168.60.166
 port: 80
 os: idSource=learned relevance=relevant type=linux
context:
 fromAttacker:

-- *CLI Output Truncated* --

triggerPacket:

-- *CLI Output Truncated* --

riskRatingValue: attackRelevanceRating=relevant
targetValueRating=medium 71
threatRatingValue: 71
interface: ge0_0
protocol: tcp

Signature: 16755/0 - Cisco Video Surveillance Stream Manager for Services Platforms and Integrated Services

Platforms DoS

```
IPS# show events alert
evIdsAlert: eventId=1238718211601194146 severity=medium vendor=Cisco
originator:
  hostId: R3-A041-IPS4240
  appName: sensorApp
  appInstanceId: 424
time: 2009/06/24 22:04:41 2009/06/24 17:04:41 CDT
signature: description=Cisco IP Camera Info Disclosure id=16733
created=20090624 type=vulnerability version=S409
  subsigId: 1
  sigDetails: Remote file access
  marsCategory: Penetrate/ViewFiles/Sensitive
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=OUT 192.168.208.63
    port: 32783
  target:
    addr: locality=OUT 192.168.60.166
    port: 80
    os: idSource=learned relevance=relevant type=linux
context:
  fromAttacker:

--      CLI Output Truncated      --

triggerPacket:

--      CLI Output Truncated      --

  riskRatingValue: attackRelevanceRating=relevant
targetValueRating=medium 71
  threatRatingValue: 71
  interface: ge0_0
  protocol: tcp
```

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 vulnerabilities that are described in this document using IPS signatures 16755/0 (Signature Name: Cisco Video Surveillance Stream Manager for Services Platforms and Integrated Services Platforms DoS), 16733/0 (Signature Name: Cisco IP Camera Info Disclosure) and 16733/1 (Signature Name: Cisco IP Camera Info Disclosure).

After the S409 dynamic signature update has been downloaded, using keyword **NR-16755/0** for IPS signature 16755/0,

NR-16733/0 for IPS signature 16733/0 or **NR-16733/1** for IPS signature 16733/1 and a query type of **All Matching Events** on the Cisco Security MARS appliance will provide a report that lists the incidents created by these IPS signatures.

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. Because MARS will not include these events in inspection rules, 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 dynamic signature updates 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 1.1	2009-June-25	Include IPS Signature S409 information
Revision 1.0	2009-June-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

- [Cisco Applied Mitigation Bulletins](#)
- [Cisco Guide to Harden Cisco IOS Devices](#)
- [Cisco Security Center](#)
- [Cisco IOS NetFlow - Home Page on Cisco.com](#)
- [Cisco IOS NetFlow White Papers](#)
- [NetFlow Performance Analysis](#)
- [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)

