

# Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco Unified Communications Manager Denial of Service Vulnerabilities

<http://www.cisco.com/warp/public/707/cisco-amb-20071017-cucm.shtml>

## Revision 1.2

Last Updated 2007 October 22 1430 UTC (GMT)

For Public Release 2007 October 17 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 *Cisco Unified Communications Manager Denial of Service Vulnerabilities* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

## Vulnerability Characteristics

There are multiple vulnerabilities in certain releases of Cisco Unified Communications Manager (CUCM), formerly Cisco Unified CallManager. These vulnerabilities are summarized in the following subsections.

**Session Initiation Protocol (SIP) INVITE UDP Denial of Service:** This vulnerability can be exploited remotely without authentication and without user interaction. Successful exploitation of this vulnerability may result in a denial of service (DoS) condition. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through SIP packets using UDP port 5060. An attacker could exploit this vulnerability through spoofing attacks. This vulnerability has been assigned CVE name CVE-2007-5537.

**Centralized Trivial File Transfer Protocol (TFTP) File Locator Service Overflow:** This vulnerability can be exploited remotely without authentication and without user interaction. Successful exploitation of this vulnerability may allow arbitrary code execution and result in a denial of service (DoS) condition. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through HTTP packets using TCP port 6970. This vulnerability has been assigned CVE name CVE-2007-5538.

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-20071017-cucm.shtml>.

## Mitigation Technique Overview

Cisco devices provide several countermeasures for the SIP INVITE UDP denial of service and Centralized TFTP File Locator Service overflow 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.

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

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

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

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

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

Effective means of exploit prevention can also be provided by the Cisco ASA 5500 Series Adaptive Security Appliance, the Cisco PIX 500 Series Security Appliance, and the Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers using the following:

- tACLs
- Unicast RPF

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

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

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

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

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 queries and event reporting.

## Risk Management

Organizations should 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 in Information Security Engagements](#) can help organizations develop repeatable security evaluation and response processes.

## Device-Specific Mitigation and Identification



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

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

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

### Cisco IOS Routers and Switches

#### Mitigation: Transit Access Control Lists

In an effort to protect the network from traffic that enters the network at ingress access points, which may include Internet connection points, partner and supplier connection points, or VPN connection

points, administrators should deploy transit access control lists (tACLs) to perform policy enforcement. Administrators can construct a tACL by explicitly permitting only authorized traffic to enter the network at ingress access points or permitting authorized traffic to transit the network in accordance with existing security policies and configurations.

The tACL policy denies unauthorized SIP packets on UDP port 5060 and HTTP packets on TCP port 6970 sent to affected devices. In the following example, 192.168.1.0/24 is the network IP address space 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 available 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 150 permit udp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 5060  
access-list 150 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 6970  
  
!  
!--- The following vulnerability-specific access control entries  
!--- (ACEs) can aid in identification of attacks  
!  
access-list 150 deny udp any 192.168.1.0 0.0.0.255 eq 5060  
access-list 150 deny tcp any 192.168.1.0 0.0.0.255 eq 6970  
  
!  
!--- Permit/deny all other Layer 3 and Layer 4 traffic in accordance  
!--- with existing security policies and configurations  
!  
!--- Explicit deny for all other IP traffic  
!  
access-list 150 deny ip any any  
  
!  
!--- Apply tACL to interfaces in the ingress direction  
  
interface GigabitEthernet0/0  
ip access-group 150 in  
  
!
```

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

## Unicast Reverse Path Forwarding

The SIP INVITE UDP denial of service vulnerability 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 SIP INVITE UDP 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 100 percent spoofing protection because spoofed packets may enter the network through a Unicast RPF-enabled interface if an appropriate return route to the source IP address exists. Administrators should take care to ensure that the appropriate Unicast RPF mode (loose or strict) is configured during the deployment of this feature because it can drop legitimate traffic that is transiting the network. In an enterprise environment, Unicast RPF might be enabled at the Internet edge and the internal access layer on the user-supporting Layer 3 interfaces.

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

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

## IP Source Guard

IP source guard (IPSG) is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering packets based on the DHCP snooping binding database and manually configured IP source bindings. Administrators can use IPSG to prevent attacks from an attacker who attempts to spoof packets by forging the source IP address and/or the MAC address. 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 SIP INVITE UDP denial of service vulnerability.

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

## Identification: Transit Access Control Lists

After the administrator applies the tACL to an interface, the **show ip access-lists** command will identify the number of SIP packets on UDP port 5060 and HTTP packets on TCP port 6970 that have been filtered. Administrators should investigate filtered packets to determine whether they are attempts to exploit these vulnerabilities. Example output for **show ip access-lists 150** follows:

```
router#show ip access-lists 150
Extended IP access list 150
 10 permit udp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 5060
 20 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 6970
 30 deny udp any 192.168.1.0 0.0.0.255 eq 5060 (12 matches)
 40 deny tcp any 192.168.1.0 0.0.0.255 eq 6970 (26 matches)
 50 deny ip any any
router#
```

In the preceding example, access list 150 has dropped **12 SIP** packets on **UDP** port **5060** for ACE sequence ID 30 and **26 HTTP** packets on **TCP** port **6970** for ACE sequence ID 40.

## Identification: Access List Logging

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



**Caution:** Access control list logging can be very CPU intensive and must be used with extreme caution. Factors that drive the CPU impact of ACL logging are log generation, log transmission, and process switching to forward packets that match log-enabled ACEs.

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

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

## Identification: Spoofing Protection Using Unicast Reverse Path Forwarding

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

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

**Note:** The **show cef interface type slot/port internal** command 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
18 verification drops
0 suppressed verification drops
router#
```

```
router#show cef drop
```

```
CEF Drop Statistics
Slot  Encap_fail  Unresolved  Unsupported  No_route  No_adj  ChkSum_Err
RP    27           0           0           18        0       0
IPv6 CEF Drop Statistics
Slot  Encap_fail  Unresolved  Unsupported  No_route  No_adj
```

```
RP          0          0          0          3          0
router#
```

```
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, allow self-ping
router#
```

```
router#show ip traffic
```

```
IP statistics:
Rcvd: 68051015 total, 2397325 local destination
      43999 format errors, 0 checksum errors, 33 bad hop count
      2 unknown protocol, 929 not a gateway
      21 security failures, 190123 bad options, 542768 with options
Opts: 352227 end, 452 nop, 36 basic security, 1 loose source route
      45 timestamp, 59 extended security, 41 record route
      53 stream ID, 3 strict source route, 40 alert, 45 cipso, 0 ump
      361634 other
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 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 Cisco Express Forwarding Forwarding Information Base.

## Cisco IOS NetFlow

### Identification: Traffic Flow Identification Using NetFlow Records

Administrators can configure Cisco IOS NetFlow on Cisco IOS routers and switches to aid in the identification of traffic flows that may be attempts to exploit the vulnerabilities described in this document. Administrators should 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 (1103375 total packets):
 1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
 .004 .434 .081 .017 .011 .033 .001 .010 .001 .000 .009 .000 .001 .001 .000
      512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
```

```

.000 .002 .380 .002 .004 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 4456704 bytes
12 active, 65524 inactive, 54766 added
3098504 aged polls, 0 flow alloc failures
Active flows timeout in 2 minutes
Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 402120 bytes
24 active, 16360 inactive, 109532 added, 54766 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	869	0.0	38	41	0.1	20.6	43.2
TCP-FTP	31	0.0	16	59	0.0	6.7	28.0
TCP-WWW	2996	0.0	12	231	0.1	8.2	11.4
TCP-other	24997	0.0	38	288	3.3	25.5	21.1
UDP-DNS	361	0.0	2	49	0.0	0.9	60.4
UDP-NTP	13982	0.0	1	76	0.0	0.8	60.5
UDP-other	10136	0.0	3	159	0.1	25.3	48.6
ICMP	556	0.0	7	68	0.0	51.4	39.6
Total:	53928	0.1	20	270	3.7	18.1	36.8

```

SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP  Pkts
Gi0/0    192.168.208.64  Gi0/1    192.168.1.21    11 13C4 13C4 1458
Gi0/0     192.16820.67     Gi0/1     192.168.150.60   06 0707 0016   80
Gi0/0    192.168.208.63  Gi0/1    192.168.1.21    06 84F2 1B3A 4
Gi0/0     192.168.14.132   Gi0/1     192.168.150.60   06 1A29 90AB   2
Gi0/0     192.168.115.113 Gi0/1     192.168.128.21   06 09BD 0017   2
Gi0/0     192.168.115.113 Local      192.168.128.20   06 0981 0017   31
Gi0/0     192.168.115.113 Gi0/1     192.168.130.41   06 0B83 01BB   30
Gi0/0     192.168.226.1    Gi0/1     192.168.206.5    11 007B 007B   1
Gi0/0     192.168.226.1    Local      192.168.128.20   11 007B 007B   1
Gi0/0     192.168.226.1    Gi0/1     192.168.128.21   11 007B 007B   1
router#

```

In the preceding example, there are multiple flows for SIP packets on UDP port 5060 (**hex value 13C4**) and HTTP packets on TCP port 6970 (**hex value 1B3A**). The UDP packets in these flows may be spoofed and may indicate an attempt to exploit the vulnerabilities described in this document. Administrators should compare these flows to baseline utilization for SIP packets on UDP port 5060 and on TCP port 6970 and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

To view only the traffic flows for SIP packets on UDP port 5060 (**hex value 13C4**), the command **show ip cache flow | include include SrcIf|\_11\_.\*13C4** will display the related NetFlow records as shown here:

```

router#show ip cache flow | include SrcIf|_11_.*13C4
SrcIf      SrcIPAddress      DstIf DstIPAddress      Pr SrcP DstP  Pkts
Gi0/0     192.168.208.64    Gi0/1 192.168.1.21     11 13C4 13C4 1458
router#

```

To view only the traffic flows for TCP port 6970 (**hex value 1B3A**), the command **show ip cache flow | include include SrcIf|\_06\_.\*1B3A** will display the related NetFlow records as shown here:

```

router#show ip cache flow | include SrcIf|_06_.*1B3A
SrcIf      SrcIPAddress      DstIf DstIPAddress      Pr SrcP DstP  Pkts

```

```
Gi0/0          192.168.208.63   Gi0/1 192.168.1.21   06 84F2 1B3A   4
router#
```

## Cisco ASA, PIX, and FWSM Firewalls

### Mitigation: Transit Access Control Lists

In an effort to protect the network from traffic that enters the network at ingress access points, which may include Internet connection points, partner and supplier connection points, or VPN connection points, administrators should deploy tACLs to perform policy enforcement. Administrators can construct a tACL by explicitly permitting only authorized traffic to enter the network at ingress access points or permitting authorized traffic to transit the network in accordance with existing security policies and configurations.

The tACL policy denies unauthorized SIP packets on UDP port 5060 and HTTP packets on TCP port 6970 sent to affected devices. In the following example, 192.168.1.0/24 is the network IP address space 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 available 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 Transit-ACL-Policy extended permit udp host 192.168.100.1 192.168.1  
access-list Transit-ACL-Policy extended permit tcp host 192.168.100.1 192.168.1  
  
!  
!--- The following vulnerability-specific access control entries  
!--- (ACEs) can aid in identification of attacks  
!  
access-list Transit-ACL-Policy extended deny udp any 192.168.1.0 255.255.255.0  
access-list Transit-ACL-Policy extended deny tcp any 192.168.1.0 255.255.255.0  
  
!  
!--- 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 Transit-ACL-Policy extended deny ip any any  
  
!  
!--- Apply tACL to interfaces in the ingress direction  
!  
access-group Transit-ACL-Policy in interface outside
```

### Mitigation: Spoofing Protection Using Unicast Reverse Path Forwarding

The SIP INVITE UDP denial of service vulnerability 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 SIP INVITE UDP 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 100 percent spoofing protection because spoofed packets may enter the network through a Unicast RPF-enabled interface if an appropriate return route to the source IP address exists. 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 SIP packets on UDP port 5060 and HTTP packets on TCP port 6970 that have been filtered. Administrators should investigate filtered packets to determine whether they are attempts to exploit these vulnerabilities. Example output for **show access-list Transit-ACL-Policy** follows:

```
firewall#show access-list Transit-ACL-Policy
access-list Transit-ACL-Policy; 5 elements
access-list Transit-ACL-Policy line 1 extended permit udp host 192.168.100.1 19
access-list Transit-ACL-Policy line 2 extended permit tcp host 192.168.100.1 19
access-list Transit-ACL-Policy line 3 extended deny udp any 192.168.1.0 255.255
access-list Transit-ACL-Policy line 4 extended deny tcp any 192.168.1.0 255.255
access-list Transit-ACL-Policy line 5 extended deny ip any any
firewall#
```

In the preceding example, the access list *Transit-ACL-Policy* has dropped **4378** SIP packets on UDP port **5060** 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 [Configuring Logging on the Cisco Security Appliance](#). Information about configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is available in [Configuring Monitoring and Logging on the Cisco FWSM](#).

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

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

```
firewall#show logging | grep 106021
Sep 20 2007 10:07:01: %ASA-4-106023: Deny udp src outside:192.168.2.18/5210 dst
  inside:192.168.1.191/5060 by access-group "Transit-ACL-Policy"
Sep 20 2007 10:07:01: %ASA-4-106023: Deny tcp src outside:192.168.3.200/3521 ds
  inside:192.168.1.33/6970 by access-group "Transit-ACL-Policy"
firewall#
```

In the preceding example, the access list *Transit-ACL-Policy* has dropped **4378** SIP packets on UDP port **5060** 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.

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

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

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

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

```
firewall#show logging | grep 106021
Sep 20 2007 10:07:01: %ASA-1-106021: Deny UDP reverse path check from 192.168.0
Sep 20 2007 10:07:01: %ASA-1-106021: Deny UDP reverse path check from 192.168.0
Sep 20 2007 10:07:01: %ASA-1-106021: Deny TCP reverse path check from 192.168.0
firewall#
```

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

```
firewall#show asp drop

Frame drop:
  Reverse-path verify failed                11
  Flow is denied by configured rule        855
```

```
Expired flow 1
Interface is down 2
```

Flow drop:

```
firewall#
```

In the preceding example, Unicast RPF has dropped **11 IP packets** received on interfaces with Unicast RPF configured.

For additional information about the configuration and use of Unicast RPF, 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 vulnerabilities described in this document. These vulnerabilities may be detected by the following signatures:

- 5912/0 - CUCM SIP INVITE UDP Denial of Service
- 5910/0 - CUCM Centralized TFTP File Locator Service Buffer Overflow

#### **5912/0 - CUCM SIP INVITE UDP Denial of Service.**

Starting with signature update S307 for sensors running Cisco IPS version 6.x or 5.x, the vulnerabilities described in this document can be detected by signature 6912/0 (Signature Name: CUCM Centralized TFTP File Locator Service Buffer Overflow). Signature 5912/0 is enabled by default, triggers a *Medium* severity event, has a signature fidelity rating (SFR) of 80, and is configured with a default event action of **Produce Alert**. Signature 5912/0 fires when multiple packets sent using UDP port 5060 are detected. Firing of this signature may indicate a potential exploit of the vulnerabilities described in this document.

#### **5910/0 - CUCM Centralized TFTP File Locator Service Buffer Overflow.**

Starting with signature update S307 for sensors running Cisco IPS version 6.x or 5.x, the vulnerabilities described in this document can be detected by signature 5910/0 (Signature Name: CUCM Centralized TFTP File Locator Service Buffer Overflow). Signature 5910/0 is enabled by default, triggers a *Medium* severity event, has an SFR of 75, and is configured with a default event action of **Produce Alert**. Signature 5910/0 fires when multiple packets sent using TCP port 6970 are detected. Firing of this signature may indicate a potential exploit of the vulnerabilities described in this document.

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

The establishment of the three-way TCP handshake is required to exploit this vulnerability, which reduces the possibility of successful attacks using spoofed IP addresses as well as false positive events for signature 5910/0.

Because UDP-based exploits can easily be spoofed, an attack that contains spoofed addresses may cause

a configured event action to inadvertently deny traffic from trusted sources. Event actions that perform blocking through ACLs or the shun command are usually configured on sensors deployed in promiscuous mode.

Cisco IPS sensors are most effective when deployed in inline protection mode combined with the use of an event action. Automatic Threat Prevention for Cisco IPS 6.x sensors deployed in inline protection mode provides threat prevention against an attack that is attempting to exploit these vulnerabilities. Threat prevention is achieved through a default override that performs an event action of **Deny Connection Inline** and **Produce Alert** for triggered signatures with a *riskRatingValue* greater than 90. Additional information about the risk rating and the calculation of its value is available in [Cisco IPS Risk Rating Explained](#).

Cisco IPS 5.x sensors deployed in inline protection mode will need to have an event action configured on a per-signature basis. Alternatively, administrators can configure an override that can perform an event action for any signatures that are triggered and are calculated as a high-risk threat. Using the **Deny Connection Inline** and **Produce Alert** event action on sensors deployed in inline protection mode provides the most effective exploit prevention.

## Identification: IPS Signature Events

### 5912/0 - CUCM SIP INVITE UDP Denial of Service.

```
IPS# show events alert
evIdsAlert: eventId=1184086129278931859 severity=medium vendor=Cisco
  originator:
    hostId: R4-IPS4240a
    appName: sensorApp
    appInstanceId: 402
  time: 2007/10/17 17:14:21 2007/10/17 12:14:21 CDT
  signature: description=CUCM SIP INVITE UDP Denial of Service id=5912 version=
    subsigId: 0
    sigDetails: CUCM SIP INVITE UDP Denial of Service
    marsCategory: DoS/Network/UDP
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.208.64
      port: 5060
    target:
      addr: locality=OUT 192.168.132.44
      port: 5060
      os: idSource=learned relevance=relevant type=linux
  triggerPacket:

!--- Packet details removed

  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 60
  threatRatingValue: 60
  interface: ge0_0
  protocol: udp
```

### 5910/0 - CUCM Centralized TFTP File Locator Service Buffer Overflow.

```
IPS# show events alert
```

```
evIdsAlert: eventId=1184086129278930978 severity=medium vendor=Cisco
originator:
  hostId: IPS
  appName: sensorApp
  appInstanceId: 402
time: 2007/10/17 17:00:57 2007/10/17 12:00:57 CDT
signature: description=CUCM Centralized TFTP File Locator Service Buffer Over
  subsigId: 0
  sigDetails: Buffer overflow in TFTP over HTTP
  marsCategory: Penetrate/BufferOverflow/Web
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=OUT 192.168.208.63
    port: 32806
  target:
    addr: locality=OUT 192.168.132.44
    port: 6970
    os: idSource=learned relevance=relevant type=linux
context:
  fromAttacker:

!--- Packet Details Removed

riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium watc
threatRatingValue: 81
interface: ge0_0
protocol: tcp
```

## Cisco Security Monitoring, Analysis, and Response System

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

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can query on events for the CUCM denial of service vulnerabilities using a query type and keyword. Using a keyword of **NR-5912/0** for IPS signature **5912/0**, which may detect the SIP INVITE UDP denial of service vulnerability; keyword of **NR-5910/0** for IPS signature **5910/0**, which may detect the centralized TFTP file locator service overflow vulnerability; and a query type of **All Matching Event Raw Messages** on the Cisco Security MARS appliance will provide a report that lists the events created by IPS signature 5912/0 or 5910/0.

The following screen shot shows the values used to query for events created by IPS signature 5912/0 (Signature Name: CUCM SIP INVITE UDP Denial of Service) or IPS signature 5910/0 (Signature Name: CUCM Centralized TFTP File Locator Service Buffer Overflow).

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

Query | Batch Query | Report | Oct 17, 2007 12:45:38 PM CDT

QUERY / REPORTS | CS-MARS Standalone: R4-MARS v4.3 Login: Administrator (pnadmin) :: Logout :: Active

View Cases | New Case

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

Query type: *Event Raw Messages ranked by Time, 0d-2h:10m* [Edit] [Clear]

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-5912/0 OR NR-5910/0	None	ANY	ANY

Apply

Specify raw message keywords:

Open (	Search String	) Close	Operation	Highlight
(	NR-5912/0	)	OR	
(	NR-5910/0	)	None	
(		)	None	
(		)	None	
(		)	None	
(		)	None	
(		)	None	
(		)	None	

Cancel | Apply

Copyright © 2003-2007 Cisco Systems, Inc. All rights reserved. | Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

The following screen shot shows the query results for **NR-5912/0 or NR-5910/0** created by the Cisco Security MARS appliance using a query type and keyword regex query.

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

Query | Batch Query | Report | Oct 17, 2007 12:55:16 PM CDT

QUERY / REPORTS | CS-MARS Standalone: R4-MARS v4.3 Login: Administrator (padmin) :: Logout :: Acti

View Cases | New Case

Load Report as On-Demand Query with Filter

Select Group... | Incident ID:  Show

Select Report... | Session ID:  Show

Query Event Data

Click the cells below to change query criteria:

Query type: *Event Raw Messages ranked by Time, 0h:10m* | Edit | Clear

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-5912/0 OR NR-5910/0	None	ANY	ANY

Save As Report | Save As Rule | Submit

Query Results

Event / Session / Incident ID	Event Type	Time	Reporting Device	Raw Message	Path / Mitigation	Tune
E:260630186, S:260630186	Unknown Device Event Type	Oct 17, 2007 12:52:47 PM CDT	R4-IPS4240a	192.168.208.64/0 --> 192.168.132.44/0 UDP Unknown Device Event Type, Time:1192643567,Risk Rating:60,VLAN:0,Port List:,0		False Positive Tuning
E:260625793, S:260625793	Unknown Device Event Type	Oct 17, 2007 12:52:33 PM CDT	R4-IPS4240a	192.168.208.64/5060 --> 192.168.132.44/5060 UDP Unknown Device Event Type, Time:1192643553,Risk Rating:60,VLAN:0,Port List:,5060		False Positive Tuning
E:260621342, S:260621342	Unknown Device Event Type	Oct 17, 2007 12:51:51 PM CDT		192.168.208.64/5060 --> 192.168.132.44/5060 UDP Unknown Device Event Type, NR-5912/0, Time:1192643511,Risk Rating:60,VLAN:0,Port List:,5060		False Positive Tuning
E:260617115, S:260617115	Unknown Device Event Type	Oct 17, 2007 12:50:33 PM CDT		192.168.208.63/32813 --> 192.168.132.44/6970 TCP Unknown Device Event Type, NR-5910/0, Time:1192643433,Risk Rating:81,VLAN:0,Port List:,6970		False Positive Tuning
E:260617062, S:260617062	Unknown Device Event Type	Oct 17, 2007 12:49:53 PM CDT		Rating:81,VLAN:0,Port List:,6970		False Positive Tuning

1 to 5 of 5 | 10 per page

Copyright © 2003–2007 Cisco Systems, Inc. | Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

## 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	2007-Oct-22	Include assigned CVE names
Revision 1.1	2007-Oct-17	Include IPS signature pack S307 information
Revision 1.0	2007-Oct-17	Initial public release

## Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html). This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

## Related Information

- [Cisco Applied Mitigation Bulletins](#)
- [Protecting Your Core: Infrastructure Protection Access Control Lists](#)
- [Transit Access Control Lists: Filtering at Your Edge](#)
- [Understanding Access Control List Logging](#)
- [Understanding Unicast Reverse Path Forwarding](#)
- [Cisco IOS NetFlow - Home Page on Cisco.com](#)
- [Cisco IOS NetFlow White Papers](#)
- [Cisco Firewall Products - Home Page on Cisco.com](#)
- [Unicast Reverse Path Forwarding Loose Mode](#)
- [Common Vulnerabilities and Exposures \(CVE\)](#) 
- [Cisco 6.x Intrusion Prevention System](#)
- [Cisco IPS Risk Rating Explained](#)
- [Cisco IPS 6.x Signature Downloads](#)
- [Cisco IPS Signatures by Release Version](#) ( [registered](#) customers only)
- [Cisco IPS Signatures by Signature ID](#) ( [registered](#) customers only)
- [Cisco Security Monitoring, Analysis, and Response System](#)

---

Help us help you.



**Please rate this document.**

- Excellent
- Good
- Average
- Fair
- Poor

**This document solved my problem.**

- Yes
- No
- Just browsing

**Suggestions for improvement:**

(256 character limit)

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

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

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