

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

Applied Mitigation Bulletins

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of Multiple Cisco Unified CallManager and Presence Server Vulnerabilities

<http://www.cisco.com/warp/public/707/cisco-amb-20070328-voip.shtml>

Revision 1.2

Last Updated 2007 April 11 1400 UTC (GMT)

For Public Release 2007 March 28 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

Cisco Unified CallManager (CUCM) and Cisco Unified Presence Server (CUPS) contain multiple vulnerabilities that may result in the failure of CUCM or CUPS functionality, resulting in a denial of service (DoS) condition:

SCCP Port Scan Denial of Service Vulnerability. This vulnerability affects only Cisco Unified CallManager. It can be exploited remotely with no authentication and no user interaction is necessary. Exploitation can allow the attacker to create a DoS condition. The attack vector is through TCP port 2000 (Skinny Call Control Protocol, SCCP) or TCP port 2443 (Secure SCCP, SCCPS). This vulnerability is not covered by a CVE ID.

ICMP Echo Request Flood Denial of Service Vulnerability. This vulnerability can be exploited remotely with no authentication and no user interaction is necessary. Exploitation can allow the attacker to create a DoS condition. The attack vector is through ICMP Type 8 (echo request) packets. This vulnerability is not covered by a CVE ID.

IPSec Manager Denial of Service Vulnerability. This vulnerability can be exploited remotely with no authentication and no user interaction is necessary. Exploitation can allow the attacker to create a DoS condition. The attack vector is through UDP port 8500. This vulnerability is not covered by a CVE ID.

This document contains information to assist Cisco customers in mitigating attempts to exploit the multiple Cisco Unified CallManager and Presence Server denial of service vulnerabilities.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisory: <http://www.cisco.com/warp/public/707/cisco-sa-20070328-voip.shtml>

Mitigation Technique Overview

Cisco devices provide several countermeasures for the multiple Cisco Unified CallManager and Presence Server vulnerabilities.

The most effective means of exploit prevention is provided by Cisco IOS Software, Cisco PIX Security Appliances, Cisco ASA Adaptive Security Appliances, and Firewall Service Modules (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers using transit access control lists (tACLs).

Cisco Intrusion Prevention System (IPS) provides detection and potential mitigation capabilities. Detective controls can also be performed using Cisco IOS NetFlow, Cisco ASA Adaptive Security Appliance, Cisco PIX Security Appliance, and the Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers through syslog messages and the counter values displayed in the **show** command output.

Additional best practices can mitigate spoofed packets that could exploit the multiple Cisco Unified CallManager and Presence Server vulnerabilities:

- Unicast Reverse Path Forwarding (Unicast RPF)
- IP Source Guard

More information about securing Unified Communications is available in the "Voice Security" section of the Unified Communications Solution Reference Network Design (SRND) for CallManager [4.x](#) or [5.x](#).

Device-Specific Mitigation and Identification



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

- [Cisco IOS Routers](#)
- [Cisco IOS Switches](#)
- [Cisco IOS NetFlow](#)

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

Cisco IOS Routers

Mitigation: Transit Access Control Lists

Transit access control lists (tACLs) can be used on Cisco IOS devices in front of vulnerable devices to mitigate the multiple Cisco Unified CallManager and Presence Server denial of service vulnerabilities.

Mitigation of the SCCP port scan denial of service vulnerability is possible by permitting TCP port 2000 (SCCP) and TCP port 2443 (SCCPS) traffic only from the IP addresses of Voice over IP (VoIP) end stations. Mitigation is facilitated when VoIP phones are deployed using a separate voice and data VLAN model. Note that there are other VoIP end stations besides the VoIP phones.

The ICMP echo request flood denial of service vulnerability can be mitigated by blocking ICMP echo messages sent to the CUCM/CUPS systems. Note that this might affect network management applications and troubleshooting procedures.

To mitigate the IPSec manager denial of service vulnerability, UDP port 8500 must be permitted only from systems that belong to the CallManager cluster. All other sources need to be blocked from accessing UDP port 8500 (with or without remote WAN clustering).

In the following sample transit ACL:

- CUCM systems are at the 192.168.138.23 and 192.168.138.24 IP addresses. They are reachable via the GigabitEthernet0/1 interface.
- The CUPS system is 192.168.138.25 and is reachable via the GigabitEthernet0/1 interface.
- VoIP endpoints are in the 192.168.128.0/24 and 192.168.150.0/24 IP address space. They are reachable via the GigabitEthernet0/0 interface.

```
ip access-list extended ACL-TRANSIT

!-- Allow SCCP and SCCPS traffic only from IP addresses assigned to
!-- Voice over IP endpoints

permit tcp 192.168.128.0 0.0.0.255 host 192.168.138.23 eq 2000
permit tcp 192.168.128.0 0.0.0.255 host 192.168.138.24 eq 2000
permit tcp 192.168.150.0 0.0.0.255 host 192.168.138.23 eq 2000
permit tcp 192.168.150.0 0.0.0.255 host 192.168.138.24 eq 2000

permit tcp 192.168.128.0 0.0.0.255 host 192.168.138.23 eq 2443
permit tcp 192.168.128.0 0.0.0.255 host 192.168.138.24 eq 2443
permit tcp 192.168.150.0 0.0.0.255 host 192.168.138.23 eq 2443
permit tcp 192.168.150.0 0.0.0.255 host 192.168.138.24 eq 2443

!-- Deny SCCP/SCCPS traffic to CUCM systems from other IP addresses

deny tcp any host 192.168.138.23 eq 2000
deny tcp any host 192.168.138.24 eq 2000

deny tcp any host 192.168.138.23 eq 2443
```

```

deny tcp any host 192.168.138.24 eq 2443

!-- Deny ICMP echo to the local CUCM and CUPS systems
!-- Note this might impact Network Management Stations
!-- and troubleshooting procedures

deny icmp any host 192.168.138.23 echo
deny icmp any host 192.168.138.24 echo
deny icmp any host 192.168.138.25 echo

!-- Block UDP port 8500 to the inside CUCM/CUPS systems from other host

deny udp any host 192.168.138.23 eq 8500
deny udp any host 192.168.138.24 eq 8500
deny udp any host 192.168.138.25 eq 8500

!-- Permit/Deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations,
!-- including other voice, transit and control protocols to CUCM/CUPS s:

!-- ACL-TRANSIT access list should be applied inbound to all
!-- non-loopback interfaces other than GigabitEthernet0/1

interface GigabitEthernet0/0
 ip access-group ACL-TRANSIT in

```

Note that **input access list** might protect devices behind the router and the router itself. In addition, **input access list** filters packets before routing takes place. When possible, **input access list** should be used instead of **output access list**.

In the Cisco Unified CallManager call processing [IP Clustering over WAN](#) deployment model, CUCM systems are deployed in multiple locations and UDP port 8500 might need to be permitted between local and remote CUCM systems. Note that CUPS does not support the WAN cluster model.

For more information on transit ACLs, refer to [Transit Access Control Lists: Filtering at Your Edge](#).

Mitigation: Anti-Spoof Protection Using Unicast Reverse Path Forwarding

The ICMP echo request flood denial of service vulnerability and IPSec Manager denial of service vulnerability may be exploited by spoofed attacks.

Protection mechanisms for anti-spoofing exist through the proper deployment and configuration of Unicast Reverse Path Forwarding (Unicast RPF). Unicast RPF is configured at the interface level and can detect and drop (discard) incoming packets with source addresses that fail the configured verification. Administrators should not rely on Unicast RPF alone to provide 100 percent spoofing protection because it will not detect subnet spoofing.

Strict mode Unicast RPF is most effective against spoofing attacks when properly deployed in close proximity to sources of spoofed packets. Strict mode Unicast RPF in Layer 3 devices coupled with IP source guard in Layer 2 devices provides the most effective means of anti-spoofing protection for

the vulnerabilities described in this document.

Care must be taken 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 transiting through the network. In an enterprise environment, Unicast RPF might be enabled at the access layer on the user-supporting Layer 3 interfaces.

Identification: Transit Access Control Lists

After the transit access control list (tACL) is applied, the **show access-lists** command can be used to identify the number of packets being filtered. Filtered packets should be investigated to determine if they are potential attempts to exploit one of the vulnerabilities described within this document. The following is an example of output for the **show access-lists ACL-TRANSIT** command:

```
Router# show access-lists ACL-TRANSIT
Extended IP access list ACL-TRANSIT
 10 permit tcp 192.168.128.0 0.0.0.255 host 192.168.138.23 eq 2000 (5 mat
 20 permit tcp 192.168.128.0 0.0.0.255 host 192.168.138.24 eq 2000 (14 ma
 30 permit tcp 192.168.150.0 0.0.0.255 host 192.168.138.23 eq 2000
 40 permit tcp 192.168.150.0 0.0.0.255 host 192.168.138.24 eq 2000
 50 permit tcp 192.168.128.0 0.0.0.255 host 192.168.138.23 eq 2443
 60 permit tcp 192.168.128.0 0.0.0.255 host 192.168.138.24 eq 2443
 70 permit tcp 192.168.150.0 0.0.0.255 host 192.168.138.23 eq 2443
 80 permit tcp 192.168.150.0 0.0.0.255 host 192.168.138.24 eq 2443
 90 deny tcp any host 192.168.138.23 eq 2000
100 deny tcp any host 192.168.138.24 eq 2000
110 deny tcp any host 192.168.138.23 eq 2443
120 deny tcp any host 192.168.138.24 eq 2443 (88 matches)
130 deny icmp any host 192.168.138.23 echo (100 matches)
140 deny icmp any host 192.168.138.24 echo (172 matches)
150 deny icmp any host 192.168.138.25 echo
160 deny udp any host 192.168.138.23 eq 8500 (26 matches)
170 deny udp any host 192.168.138.24 eq 8500 (35 matches)
180 deny udp any host 192.168.138.25 eq 8500
```

In the preceding example, there were 5 and 14 TCP port 2000 packets, 100 and 172 ICMP echo messages, and 26 and 35 UDP port 8500 packets dropped by access list ACL-TRANSIT to CUCM servers 192.168.138.23 and 192.168.138.24 respectively.

Identification: Anti-Spoof Protection Using Unicast Reverse Path Forwarding

With Unicast RPF properly deployed and configured throughout the network infrastructure, the **show ip interface *interfacetype slot/port***, **show cef *interfacetype slot/port* internal**, and **show ip traffic** commands can be used to identify the number of packets that Unicast RPF has discarded.

```
Router# show ip interface GigabitEthernet0/0
GigabitEthernet0/0 is up, line protocol is up

<Output suppressed>

IP verify source reachable-via RX, allow default
 2023 verification drops
 0 suppressed verification drops
IP multicast multilayer switching is disabled

Router# show cef interface GigabitEthernet0/0 internal
GigabitEthernet0/0 is up (if_number 95)

<Output suppressed>
```

Subblocks:

```
ip verify: via=rx (allow default), acl=0, drop=2023, sdrop=0
```

```
Router# show ip traffic | include RPF
      25 no route, 7236 unicast RPF, 0 forced drop
```

In the preceding examples, Unicast RPF has dropped 2023 IP packets received on interface GigabitEthernet0/0 due to the inability to verify the source address of the IP packets within the Cisco Express Forwarding (CEF) Forwarding Information Base (FIB). The total number of packets discarded in all interfaces because they failed Unicast RPF verification is 7236.

Cisco IOS Switches

Mitigation: Anti-Spoof Protection Using IP Source Guard

The ICMP echo request flood denial of service vulnerability and IPSec Manager denial of service vulnerability may be exploited by spoofed attacks.

Protection mechanisms for anti-spoofing exist through the proper deployment and configuration of IP source guard. IP source guard is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. IP source guard can be used to help prevent attacks from a malicious user who attempts to spoof packets by forging the source IP address and/or the MAC address. When properly deployed and configured, IP source guard coupled with strict mode Unicast RPF provides the most effective means of anti-spoofing protection for the ICMP echo request flood denial of service vulnerability and IPSec Manager denial of service vulnerability.

After IP source guard is enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping. After a DHCP IP address is assigned, a port access control list (port ACL) is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic.

The IP source binding table has bindings that are learned by DHCP snooping or manually configured (static IP source bindings). An entry in this table has an IP address, its associated MAC address, and its associated VLAN number. The switch uses the IP source binding table only when IP source guard is enabled.

IP source guard is supported only on Layer 2 ports, including access and trunk ports. IP source guard can be configured for source IP address filtering or with source IP and MAC address filtering.

Additional information about IP source guard is available at [Configuring DHCP Features and IP Source Guard](#).

Cisco IOS NetFlow

Identification

In the case of the SCCP port acan denial of service vulnerability, traffic information from Cisco IOS NetFlow needs to be reviewed to identify anomalous sources of TCP port 2000 (SCCP, hex value 07D0) and TCP port 2443 (SCCPS, hex value 098B).

For the ICMP echo request flood denial of service vulnerability, note that NetFlow indicates the ICMP echo request type and code as the "Destination Port," that is, "0800" is displayed (Type 8,

Code 0).

For the IPSec Manager denial of service vulnerability, NetFlow can be used to identify traffic to UDP port 8500 (hex value 2134). In the following example, ICMP echo messages with a source IP address of 192.168.160.107 are sent to CUCM/CUPS systems 192.168.138.23 and 192.168.138.24

```
Router# show ip cache flow | include DstP|07D0|098B|0800|2134
SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr SrcP DstP  Pk
Gi0/0     192.168.160.132 Gi0/1      192.168.138.23 06 1C85 07D0
Gi0/0     192.168.160.195 Gi0/1      192.168.138.24 06 1D32 07D0
Gi0/0     192.168.160.134 Gi0/1      192.168.138.23 06 1A57 07D0
Gi0/0     192.168.160.110 Gi0/1      192.168.138.24 06 20CA 098B
Gi0/0     192.168.160.110 Gi0/1      192.168.138.24 06 2038 098B
Gi0/0     192.168.160.110 Gi0/1      192.168.138.24 06 18FB 07D0
Gi0/0     192.168.160.105 Gi0/1      192.168.138.24 01 0000 0800
Gi0/0     192.168.160.107 Gi0/1      192.168.138.24 01 0000 0800
Gi0/0     192.168.160.107 Gi0/1      192.168.138.23 01 0000 0800
Gi0/0     192.168.132.45  Gi0/1      192.168.138.24 11 19BB 2134
Gi0/0     192.168.132.44  Gi0/1      192.168.138.23 11 190A 2134
```

Cisco ASA, PIX, and FWSM Firewalls

Mitigation: Transit Access Control Lists

Transit access control lists (tACLs) can be used on FWSM or ASA devices in front of the vulnerable devices to mitigate the multiple Cisco Unified CallManager and Presence Server denial of service vulnerabilities.

Mitigation of the SCCP port scan denial of service vulnerability is possible by permitting TCP port 2000 (SCCP) and TCP port 2443 (SCCPS) traffic only from the IP addresses of Voice over IP (VoIP) end stations. Mitigation is facilitated when VoIP phones are deployed using a separate voice and data VLAN model. Note that there are other VoIP end stations besides the VoIP phones.

The ICMP echo request flood denial of service vulnerability can be mitigated by blocking ICMP echo messages to the CUCM/CUPS systems. Note that this might affect network management applications and troubleshooting procedures. In the Cisco Unified CallManager call processing [IP clustering over WAN](#) deployment model, CUCM systems are deployed in multiple locations.

To mitigate the IPSec Manager denial of service vulnerability, UDP port 8500 needs to be permitted to and from remote CUCM systems. All other sources need to be blocked from accessing UDP port 8500 (with or without remote WAN clustering).

In the following sample transit ACL:

- CUCM systems are at the 192.168.138.23 and 192.168.138.24 IP addresses. They are reachable via the inside interface.
- The CUPS system is 192.168.138.25 and is reachable via the inside interface.
- VoIP endpoints are in the 192.168.128.0/24 and 192.168.150.0/24 IP address space. They are reachable via the outside interface.

Note that the access list uses the [object grouping feature](#), which simplifies the construction of the access list by assigning a name to a list of one or more IP addresses or IP address blocks. Then those named groups can be used in an access control entry (ACE) and the administrator does not have to enter an ACE for each IP address or IP address block separately. The firewall will expand the group ACE into the individual entries that will be seen in the **show access-list** command output. First the groups are defined:

```
!-- Network object group for CUCM systems that face the inside interface
```

```
object-group network OBJ-INSIDE-CUCM
```

```
!-- list each of the IP addresses of CUCM systems
```

```
network-object host 192.168.138.23
network-object host 192.168.138.24
```

```
object-group network OBJ-INSIDE-CUCM-CUPS
```

```
!-- list each of the IP addresses of both CUCM and CUPS systems
```

```
network-object host 192.168.138.23
network-object host 192.168.138.24
network-object host 192.168.138.25
```

```
!-- Network object group of endpoints facing the outside interface
```

```
object-group network OBJ-OUTSIDE-ENDPOINT
```

```
!-- List the IP address or IP address blocks that contain VoIP endpoints.
```

```
network-object 192.168.128.0 255.255.255.0
network-object 192.168.150.0 255.255.255.0
```

After the groups are defined, they can be used in the access list:

```
!-- Allow SCCP and SCCPS traffic only from IP addresses assigned to  
!-- Voice over IP endpoints
```

```
access-list ACL-OUTSIDE extended permit tcp object-group OBJ-OUTSIDE-ENDPOIN  
object-group OBJ-INSIDE-CUCM eq 2000  
access-list ACL-OUTSIDE extended permit tcp object-group OBJ-OUTSIDE-ENDPOIN  
object-group OBJ-INSIDE-CUCM eq 2443
```

```
!-- Deny SCCP/SCCPS traffic to CUCM systems from other IP addresses
```

```
access-list ACL-OUTSIDE extended deny tcp any object-group OBJ-INSIDE-CUCM e  
access-list ACL-OUTSIDE extended deny tcp any object-group OBJ-INSIDE-CUCM e
```

```
!-- Deny ICMP echo to the local CUCM and CUPS systems  
!-- Note this might impact Network Management Stations and troubleshooting p
```

```
access-list ACL-OUTSIDE extended deny icmp any object-group OBJ-INSIDE-CUCM-
```

```
!-- Block UDP port 8500 to the inside CUCM/CUPS systems from other hosts
```

```

access-list ACL-OUTSIDE extended deny udp any object-group OBJ-INSIDE-CUCM-C

!-- Permit/Deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations,
!-- including other voice, transit and control protocols to CUCM/CUPS system

!-- Apply access-list to outside interface

access-group ACL-OUTSIDE in interface outside

```

Identification: Transit Access Control Lists

In the following example, all CUCM/CUPS systems are facing the inside interface and the **show access-list** command indicates that 42 packets were blocked for the 192.168.138.23 CUCM/CUPS system. For each of the ACEs that have at least one object group, the ACE is listed first as configured with the group name, then the expanded ACEs are listed with the same ACE line number.

```

Firewall# show access-list ACL-OUTSIDE
access-list ACL-OUTSIDE; 19 elements
access-list ACL-OUTSIDE line 1 extended permit tcp object-group OBJ-OUTSIDE-
object-group OBJ-INSIDE-CUCM eq 2000 0xd054f5da
access-list ACL-OUTSIDE line 1 extended permit tcp 192.168.128.0 255.255.255
192.168.138.23 eq 2000 (hitcnt=0) 0xl28c3c9f
access-list ACL-OUTSIDE line 1 extended permit tcp 192.168.128.0 255.255.255
192.168.138.24 eq 2000 (hitcnt=0) 0xd7f06535
access-list ACL-OUTSIDE line 1 extended permit tcp 192.168.150.0 255.255.255
192.168.138.23 eq 2000 (hitcnt=0) 0x5338ccad
access-list ACL-OUTSIDE line 1 extended permit tcp 192.168.150.0 255.255.255
192.168.138.24 eq 2000 (hitcnt=0) 0xd281b603
access-list ACL-OUTSIDE line 2 extended permit tcp object-group OBJ-OUTSIDE-
object-group OBJ-INSIDE-CUCM eq 2443 0xb260844
access-list ACL-OUTSIDE line 2 extended permit tcp 192.168.128.0 255.255.255
192.168.138.23 eq 2443 (hitcnt=0) 0xd0987243
access-list ACL-OUTSIDE line 2 extended permit tcp 192.168.128.0 255.255.255
192.168.138.24 eq 2443 (hitcnt=0) 0x16665ff8
access-list ACL-OUTSIDE line 2 extended permit tcp 192.168.150.0 255.255.255
192.168.138.23 eq 2443 (hitcnt=0) 0x58603227
access-list ACL-OUTSIDE line 2 extended permit tcp 192.168.150.0 255.255.255
192.168.138.24 eq 2443 (hitcnt=0) 0xfd3e1a80
access-list ACL-OUTSIDE line 3 extended deny tcp any object-group OBJ-INSIDE
eq 2000 0xf677709d
access-list ACL-OUTSIDE line 3 extended deny tcp any host 192.168.138.23 eq
(hitcnt=0) 0xdb0430ba
access-list ACL-OUTSIDE line 3 extended deny tcp any host 192.168.138.24 eq
(hitcnt=0) 0xad1014ee
access-list ACL-OUTSIDE line 4 extended deny tcp any object-group OBJ-INSIDE
eq 2443 0x6734cf27
access-list ACL-OUTSIDE line 4 extended deny tcp any host 192.168.138.23 eq
(hitcnt=0) 0x37843dd4
access-list ACL-OUTSIDE line 4 extended deny tcp any host 192.168.138.24 eq
(hitcnt=0) 0x2eece9b2
access-list ACL-OUTSIDE line 5 extended deny icmp any object-group
OBJ-INSIDE-CUCM-CUPS echo 0xc8d47a18
access-list ACL-OUTSIDE line 5 extended deny icmp any host 192.168.138.23 ec:
(hitcnt=42) 0x63d46eca
access-list ACL-OUTSIDE line 5 extended deny icmp any host 192.168.138.24 ec:
(hitcnt=0) 0x7491f7e1
access-list ACL-OUTSIDE line 5 extended deny icmp any host 192.168.138.25 ec:

```

```

        (hitcnt=0) 0xfe6871cf
access-list ACL-OUTSIDE line 6 extended deny udp any object-group
OBJ-INSIDE-CUCM-CUPS eq 8500 0xb35f3669
access-list ACL-OUTSIDE line 6 extended deny udp any host 192.168.138.23 eq
(hitcnt=0) 0x2fc70d6d
access-list ACL-OUTSIDE line 6 extended deny udp any host 192.168.138.24 eq
(hitcnt=0) 0x187b4431
access-list ACL-OUTSIDE line 6 extended deny udp any host 192.168.138.25 eq
(hitcnt=0) 0xbf1c1b4c

```

In the preceding example, 42 UDP port 8500 packets to 192.168.138.23 were denied.

Identification: Firewall Syslog Messages

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

In the following examples, the **show logging | include regex** command is used to extract syslog messages from the logging buffer on the firewall.

```

FWSM# show logging | include 106023
Mar 16 2007 20:58:35: %FWSM-4-106023: Deny udp src outside:192.168.160.132/5
dst inside:192.168.138.23/8500 by access-group "ACL-OUTSIDE" [0xb19538ff, 0x

```

Cisco Intrusion Prevention System

The Cisco Intrusion Prevention System (IPS) appliances and services modules can be used to provide threat detection and prevention against attempts to exploit vulnerabilities described in this document.

Potential exploits of the ICMP echo request flood denial of service vulnerability can be detected with signature 6902/0 (Signature Name: Net Flood ICMP Request), starting with signature pack S4. The signature 6902/0 alarm severity defaults to Informational because it might result in false positives.

Starting with signature update S278 for sensors running Cisco IPS version 6.x or 5.x, the IPSec Manager Denial of Service Vulnerability described in this document can be detected by signature 5854/0 (Signature Name: Cisco CUCM/CUPS Denial of Service Vulnerability). Signature 5854/0 is enabled by default and triggers a Medium severity event (see the example later in this section).

Identification: IPS Signatures

IPS signature 5854/1 (Signature Name: Cisco CUCM/CUPS Denial of Service Vulnerability) triggers a medium severity alarm on potential attempts to exploit the SCCP Port Scan Denial of Service vulnerability, which may indicate an attempt to denial service offered by the affected platform. The following medium severity event was triggered by signature 5854/1 after a potential attempt to exploit the vulnerability.

```

Sensor6x# show events alert | include id=5854
evIdsAlert: eventId=1166761098236251265 severity=medium vendor=Cisco
originator:
hostId: R4-IPS4240a
appName: sensorApp
appInstanceId: 380
time: 2007/04/11 05:15:33 2007/04/11 00:15:33 CDT
signature: description=Cisco CUCM/CUPS Denial of Service Vulnerability
id=5854 version=S279

```

```

    subsigId: 1
    sigDetails: SCCP Port Scan Denial of Service Vulnerability
    marsCategory: DoS/MiscServer
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=OUT 192.168.208.63
    port: 34917
  target:
    addr: locality=OUT 192.168.132.44
    port: 2000
    os: idSource=unknown relevance=relevant type=unknown
context:
  fromAttacker:

```

!--- Output suppressed

```
triggerPacket:
```

!--- Output suppressed

```

riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 5
threatRatingValue: 56
interface: ge0_0
protocol: tcp

```

The following *Informational* severity event was triggered by signature 6902/0 (Signature Name: Net Flood ICMP Request) after a potential attempt to exploit the ICMP echo request flood denial of service vulnerability.

```
IPS# show events alert past 00:10:00 | include id=6902
```

```

evIdsAlert: eventId=1166747458239518346 severity=informational vendor=Cisco
originator:
  hostId: R4-IPS4240a
  appName: sensorApp
  appInstanceId: 480
time: 2007/03/24 04:15:24 2007/03/23 23:15:24 CDT
signature: description=Net Flood ICMP Request id=6902 version=S4
  subsigId: 0
  marsCategory: DoS/Network/ICMP
interfaceGroup: vs0
vlan: 0
participants:
alertDetails: MaxPPS during this interval: 5328 ;
riskRatingValue: targetValueRating=medium 25
threatRatingValue: 25
interface: sy0_0
protocol: icmp

```

Notice that the default Target Value Rating of 25 will cause a low [risk rating](#) to be evaluated for this event.

Signature 6902/0 is disabled by default. It can be enabled as follows:

```

IPS# configure terminal
IPS(config)# service signature-definition sig0
IPS(config-sig)# signatures 6902 0
IPS(config-sig-sig)# status
IPS(config-sig-sig-sta)# enabled true

```

```

IPS(config-sig-sig-sta)# exit
IPS(config-sig-sig)# exit
IPS(config-sig)# exit
Apply Changes?[yes]: yes
IPS(config)# exit

```

The following Medium severity event was triggered on a Cisco IPS sensor deployed in promiscuous mode.

IPS signature 5854/0 (Signature Name: Cisco CUCM/CUPS Denial of Service Vulnerability) triggers a medium severity alarm on potential attempts to exploit the IPsec Manager Denial of Service vulnerability., which may indicate an attempt to deny service offered by the affected platform. The following medium severity event was triggered by signature 5854/0 after a potential attempt to exploit the vulnerability.

```

Sensor6x# show events alert | include id=5854
evIdsAlert: eventId=1166754278236272652 severity=medium vendor=Cisco
originator:
  hostId: Sensor6x
  appName: sensorApp
  appInstanceId: 7007
time: 2007/03/30 17:25:02 2007/03/30 12:25:02 CDT
signature: description=Cisco CUCM/CUPS Denial of Service Vulnerability id
          version=S278
  subSigId: 0
  sigDetails: IPsec Manager Denial of Service Vulnerability
  marsCategory: DoS/MiscServer
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=OUT 192.168.160.193
    port: 1865
  target:
    addr: locality=OUT 192.168.138.24
    port: 8500
    os: idSource=unknown relevance=relevant type=unknown
triggerPacket:

  <Output suppressed>

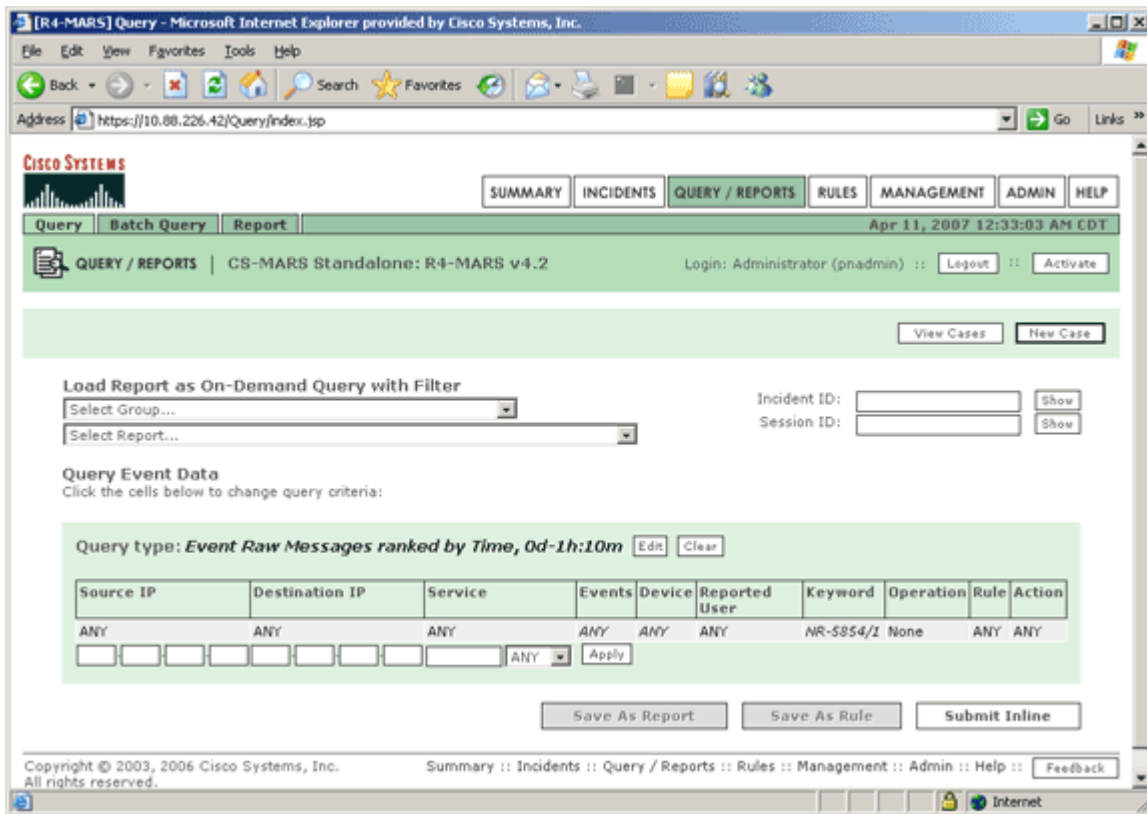
riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 5
threatRatingValue: 56
interface: ge0_1
protocol: udp

```

Cisco Security Monitoring, Analysis, and Response System

Identification: SCCP Port Scan Denial of Service Vulnerability

The following query will show events triggered by signature 5854/1 that could be associated with attempts to exploit this vulnerability. Note the query is with *All Matching Element Raw Messages* result format and keyword equal to *NR-5854/1*.



The following display is the result of the previous query.

The screenshot shows the Cisco Security MARS console interface. The browser window title is "[R4-MARS] Query Results - Microsoft Internet Explorer provided by Cisco Systems, Inc.". The address bar shows the URL: "https://10.88.226.42/Query/QuerySubmit.jsp?ResubmitAndClearFaging=true&inlineReport=1".

The console has a navigation menu with tabs: SUMMARY, INCIDENTS, QUERY / REPORTS (selected), RULES, MANAGEMENT, ADMIN, HELP. Below the menu, there are buttons for "View Cases" and "New Case".

The main content area is titled "Query Event Data" and includes a section for "Load Report as On-Demand Query with Filter". It has dropdown menus for "Select Group..." and "Select Report...". There are also input fields for "Incident ID:" and "Session ID:" with "Show" buttons.

The "Query type" is set to "Event Raw Messages ranked by Time, 0d-1h:10m". Below this is a table of query criteria:

| Source IP | Destination IP | Service | Events | Device | Reported User | Keyword | Operation | Rule | Action |
|-----------|----------------|---------|--------|--------|---------------|-----------|-----------|------|--------|
| ANY | ANY | ANY | ANY | ANY | ANY | NR-5854/1 | None | ANY | ANY |

Buttons for "Save As Report", "Save As Rule", and "Submit" are located below the criteria table.

The "Query Results" section displays a table of event data:

| Event / Session / Incident ID | Event Type | Time | Reporting Device | Raw Message | Path / Mitigation | Tune |
|-------------------------------|-------------------------------|------------------------------|------------------|---|-------------------|----------------|
| E:16166356, S:16166356 | Unknown Device Event Type [a] | Apr 11, 2007 12:27:22 AM CDT | R4-IPS4240a | 192.168.208.63/0 --> 0.0.0.0/0 TCP Unknown Device Event Type: [REDACTED], Time:1176269242, Risk Rating:46, VLAN:0, Port List:0 | [REDACTED] | False Positive |
| E:16166221, S:16166221 | Unknown Device Event Type [a] | Apr 11, 2007 12:27:07 AM CDT | R4-IPS4240a | 192.168.208.63/34921 --> 192.168.132.44/2000 TCP Unknown Device Event Type: [REDACTED], Time:1176269227, Risk Rating:56, VLAN:0, Port List:2000 | [REDACTED] | False Positive |
| E:16164959, S:16164959 | Unknown Device Event Type [a] | Apr 11, 2007 12:19:15 AM CDT | R4-IPS4240a | 192.168.208.63/34920 --> 192.168.132.44/2000 TCP Unknown Device Event Type: [REDACTED], Time:1176268755, Risk Rating:56, VLAN:0, Port List:2000 | [REDACTED] | False Positive |

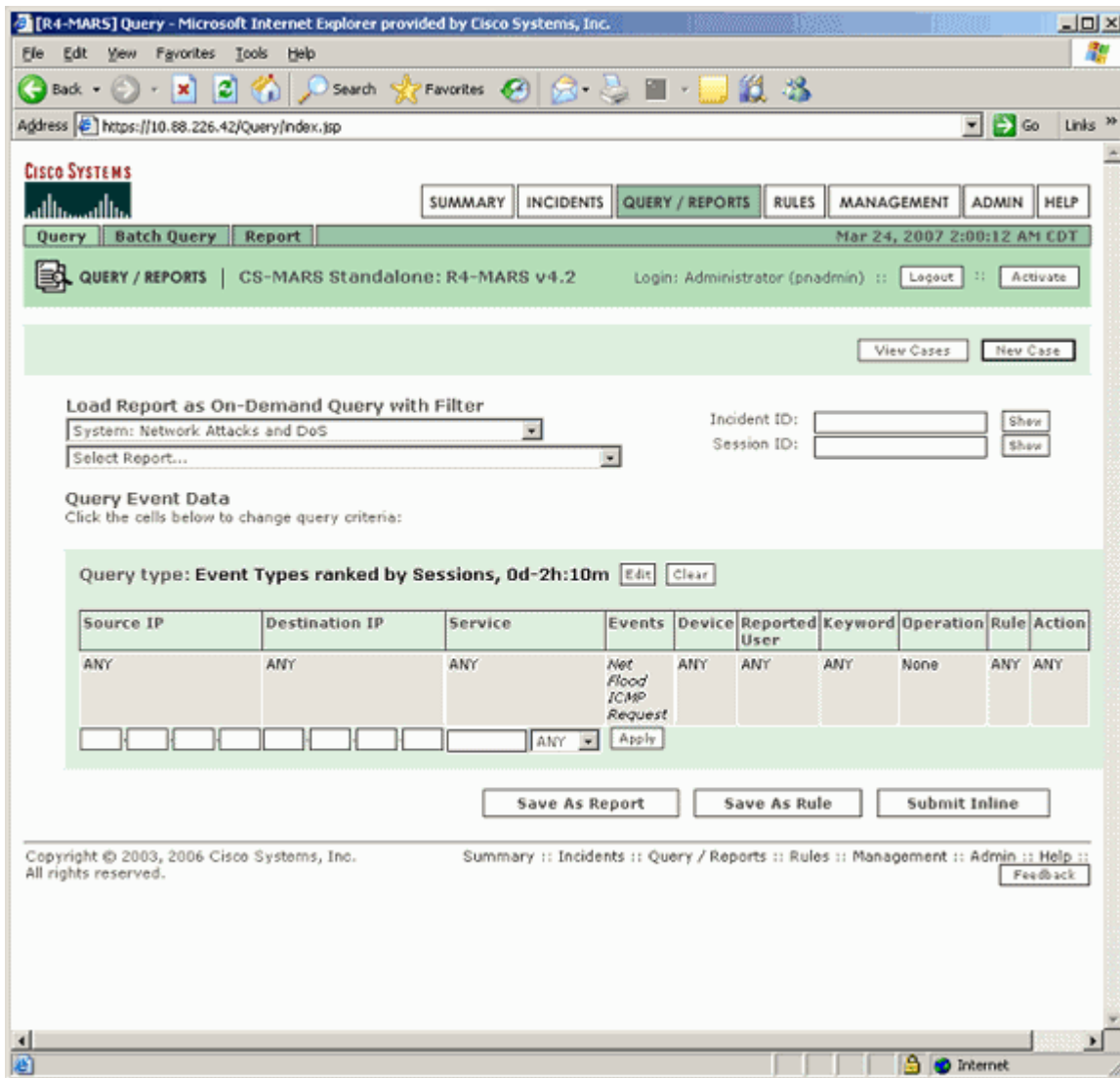
At the bottom of the results table, it shows "1 to 3 of 3" and "25 per page".

The footer of the console includes the copyright notice: "Copyright © 2003, 2006 Cisco Systems, Inc. All rights reserved." and a navigation menu: "Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help :: Feedback".

Identification: ICMP Echo Request Flood Denial of Service Vulnerability

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) console can be monitored for attempts to exploit the ICMP echo request flood denial of service vulnerability.

The following query will show events triggered by signatures that could be associated with attempts to exploit this vulnerability.



The following display is the result of the previous query.

CISCO SYSTEMS

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

Query Batch Query Report Mar 24, 2007 2:01:20 AM CDT

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

View Cases New Case

Load Report as On-Demand Query with Filter

System: Network Attacks and DoS Incident ID: Show

Select Report... Session ID: Show

Query Event Data

Click the cells below to change query criteria:

Query type: Event Types ranked by Sessions, 0d-2h:10m Edit Clear

| Source IP | Destination IP | Service | Events | Device | Reported User | Keyword | Operation | Rule | Action |
|-----------|----------------|---------|------------------------|--------|---------------|---------|-----------|------|--------|
| ANY | ANY | ANY | Net Flood ICMP Request | ANY | ANY | ANY | None | ANY | ANY |

Save As Report Save As Rule Submit

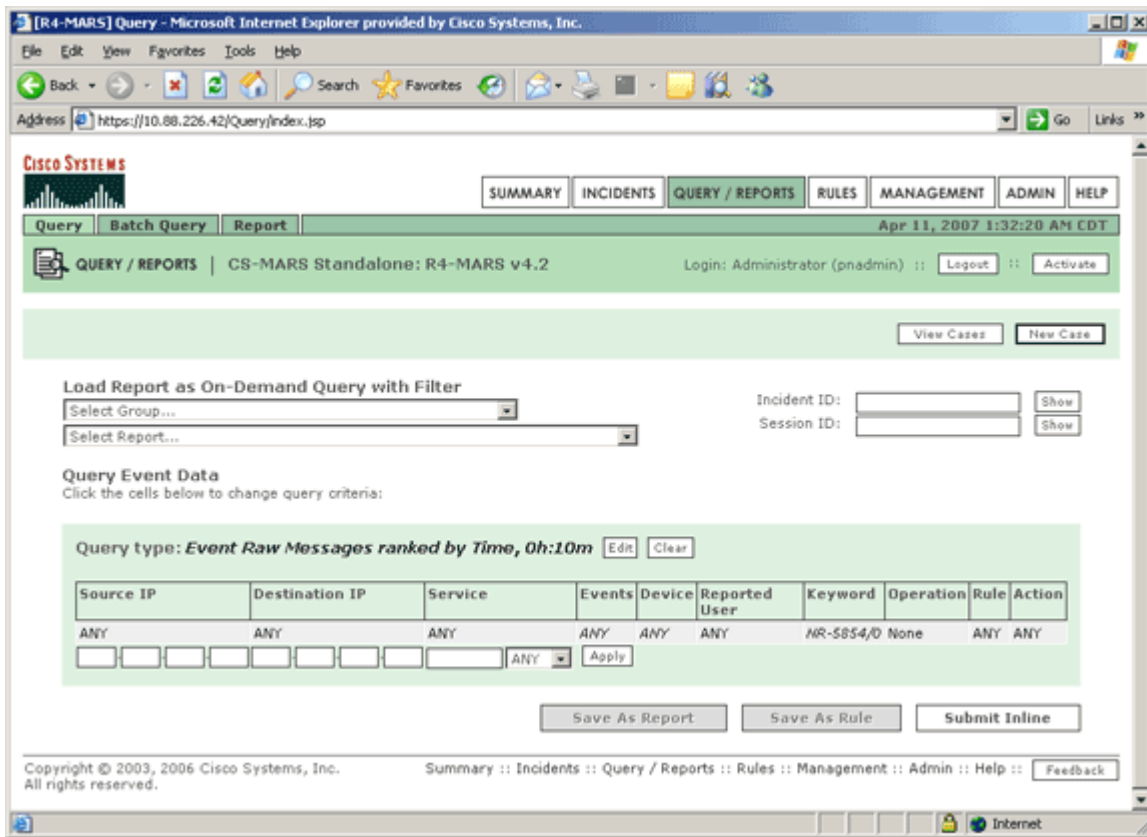
Query Results

| Rank | Count (# of Sessions) | Event ID | Description | CVE Name | Severity | Device Event ID | Groups |
|------|-----------------------|----------|------------------------|----------|----------|---|---------------------------|
| 1 | 240 | 1906902 | Net Flood ICMP Request | | | Cisco IDS 3.1: NR-6902/0: Cisco MySDN IPS Signatures, Cisco IDS 4.0: NR-6902/0: Cisco MySDN IPS Signatures, Cisco IOS 12.2: NR-6902/0: Cisco MySDN IPS Signatures, Cisco IPS 5.x: NR-6902/0: Cisco MySDN IPS Signatures | DoS/All, DoS/Network/ICMP |

Total Sessions: 240

Identification: IPSec Manager Denial of Service Vulnerability

The following query will show events triggered by signatures that could be associated with attempts to exploit this vulnerability. Note the query is with *All Matching Element Raw Messages* result format and keyword *NR-5854/0*.



The following display is the result of the previous query.

Copyright © 2003, 2006 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help :: Feedback

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-April-11 | Included information about signature pack S279 in IPS Signatures and CS-MARS sections. |
| Revision 1.1 | 2007-March-30 | Included information about S278 signature in IPS Signatures and CS-MARS sections. |
| Revision 1.0 | 2007-March-28 | 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

- ["Voice Security" section of the Unified Communications SRND for CallManager 4.x](#)
- ["Voice Security" section of the Unified Communications SRND for CallManager 5.x](#)
- [Cisco CallManager TCP and UDP Port Usage](#)
- [Cisco CallManager IP Clustering over WAN](#)
- [Cisco Security Appliance System Log Messages](#)
- [Transit Access Control Lists: Filtering at Your Edge](#)
- [Cisco IPS 6.x Signature Downloads](#) ([registered](#) customers only)
- [Cisco IPS Signatures by Release Version](#) ([registered](#) customers only)
- [Cisco Unified Presence Server Cluster](#)

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.](#)