

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco Unified IP Phone Overflow and Denial of Service Vulnerabilities

Document ID: 100637

<http://www.cisco.com/warp/public/707/cisco-amb-20080213-phone.shtml>

Revision 1.1

Last Updated 2008 February 15 1600 UTC (GMT)

For Public Release 2008 February 13 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

[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 IP Phone Overflow and 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 Cisco Unified IP Phone 7906G, 7911G, 7935, 7936, 7940, 7940G, 7941G, 7960, 7960G, 7961G, 7970G, and 7971G devices running various versions of Skinny Client Control Protocol (SCCP) firmware and Cisco Unified IP Phone 7940, 7940G, 7960, and 7960G devices running various versions of Session Initiation Protocol (SIP) firmware. These following subsections summarize these vulnerabilities:

Vulnerabilities Affecting Cisco Unified IP Phones Running SCCP Firmware

Large ICMP Echo Request Denial of Service: This vulnerability can be exploited remotely without authentication and without end-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 an ICMP ECHO packet. An attacker could exploit this vulnerability using spoofed packets. This vulnerability has been assigned CVE identifier CVE-2008-0526.

DNS Response Parsing Overflow: This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may allow arbitrary code execution. The attack vector for exploitation is through DNS packets using UDP port 53. An attacker could exploit this vulnerability using spoofed packets. Due to the nature of this vulnerability, packet filtering mitigations will not be discussed. This vulnerability has been assigned CVE identifier CVE-2008-0530.

HTTP Server Denial of Service: This vulnerability can be exploited remotely without authentication and without end-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 HTTP packets using TCP port 80. This vulnerability has been assigned CVE identifier CVE-2008-0527.

SSH Server Denial of Service: This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may result in a denial of service (DoS) condition or allow arbitrary code execution. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through SSH packets using TCP port 22. This vulnerability has been assigned CVE identifier CVE-2004-2486.

Vulnerabilities Affecting Cisco Unified IP Phones Running SIP Firmware

SIP MIME Boundary Overflow: This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may allow arbitrary code execution. The attack vector for exploitation is through SIP packets using TCP port 5060 or UDP port 5060. An attacker could exploit this vulnerability using spoofed packets. This vulnerability has been assigned CVE identifier CVE-2008-0528.

Telnet Server Overflow: This vulnerability can be exploited remotely with authentication and without end-user interaction. Successful exploitation of this vulnerability may allow an authenticated unprivileged user to obtain privileged access. The attack vector for exploitation is through Telnet packets using TCP port 23. This vulnerability has been assigned CVE identifier CVE-2008-0529.

DNS Response Parsing Overflow: This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may allow arbitrary code execution. The attack vector for exploitation is through DNS packets using UDP port 53. An attacker could exploit this vulnerability using spoofed packets. Due to the nature of this vulnerability packet filtering mitigations will not be discussed. This vulnerability has been assigned CVE identifier CVE-2008-0530.

SIP Proxy Response Overflow: This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may allow arbitrary code execution. The attack vector for exploitation is through SIP packets using TCP port 5060 or UDP port 5060. An attacker could exploit this vulnerability using spoofed packets. This vulnerability has been assigned CVE identifier CVE-2008-0531.

Vulnerable, non-affected, and fixed software information is available in the PSIRT Security Advisory: <http://www.cisco.com/warp/customer/707/cisco-sa-20080213-phone.shtml>.

Mitigation Technique Overview

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

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

- 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 with a network attack vector.

The proper deployment and configuration of Unicast RPF provides an effective means of protection against attacks that use packets with spoofed source IP addresses. Unicast RPF should be deployed as close to all traffic sources as possible.

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

Effective means of exploit prevention can also be provided by Cisco ASA 5500 Series Adaptive Security Appliance, 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 with a network attack vector.

Effective use of Cisco Intrusion Prevention System (IPS) event actions provides visibility into and protection against attacks that attempt to exploit the vulnerabilities discussed later in this document.

Cisco IOS NetFlow can provide visibility into network-based 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.

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 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

Vulnerabilities Affecting Cisco Unified IP Phones Running SSCP Firmware

To protect the network from traffic entering at ingress access points, which may include Internet connection points, partner and supplier connection points, or VPN connection points, administrators are advised to 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. A tACL workaround cannot provide complete protection against vulnerabilities with a network attack vector when the attack originates from a trusted source address.

The tACL policy denies unauthorized ICMP Echo Requests, HTTP packets on TCP port 80 (www), and SSH packets on TCP port 22 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 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 and protocols
!

access-list 150 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 echo
access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq www
access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 22

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

access-list 150 deny icmp any 192.168.60.0 0.0.0.255 echo
access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq www
access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 22

!
!-- 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
```

Vulnerabilities Affecting Cisco Unified IP Phones Running SIP Firmware

This tACL policy denies unauthorized SIP packets on TCP port 5060 and UDP port 5060 and Telnet packets on TCP port 23. 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 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 and protocols
!

access-list 150 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq telnet

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

access-list 150 deny udp any 192.168.60.0 0.0.0.255 eq 5060
access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 5060
access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq telnet

!
!-- 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**.

Mitigation: Spoofing Protection

Unicast Reverse Path Forwarding

The vulnerabilities described in this document with a network attack vector can be exploited via spoofed IP packets. The proper deployment and configuration of Unicast Reverse Path Forwarding (Unicast RPF) can provide protection mechanisms for spoofing related to the following vulnerabilities:

Vulnerabilities Affecting Cisco Unified IP Phones Running SCCP Firmware

- Large ICMP Echo Request Denial of Service
- DNS Response Parsing Overflow

Vulnerabilities Affecting Cisco Unified IP Phones running SIP firmware

- SIP Proxy Response Overflow
- SIP MIME Boundary Overflow
- DNS Response Parsing Overflow

Unicast RPF is configured at the interface level and can detect and drop packets that lack a verifiable source IP address. Administrators should not rely on Unicast RPF to provide complete spoofing protection, because spoofed packets may enter the network through a Unicast RPF-enabled interface if an appropriate return route to the source IP address exists. Administrators are advised to take care to ensure that the appropriate Unicast RPF mode (loose or strict) is configured during the deployment of this feature because it can drop legitimate traffic that is transiting the network. In an enterprise environment, Unicast RPF might be enabled at the Internet edge and the internal access layer on the user-supporting Layer 3 interfaces.

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

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

IP Source Guard

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

Vulnerabilities Affecting Cisco Unified IP Phones Running SCCP Firmware

- Large ICMP Echo Request Denial of Service
- DNS Response Parsing Overflow

Vulnerabilities Affecting Cisco Unified IP Phones Running SIP Firmware

- SIP Proxy Response Overflow
- SIP MIME Boundary Overflow
- DNS Response Parsing Overflow

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

Identification: Transit Access Control Lists

Vulnerabilities Affecting Cisco Unified IP Phones Running SCCP Firmware

After the administrator applies the tACL to an interface, the **show ip access-lists** command will identify the number of ICMP Echo Requests, HTTP packets on TCP port 80 (www), and SSH packets on TCP port 22 that have been filtered. Administrators are advised to 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 icmp host 192.168.100.1 192.168.60.0 0.0.0.255 echo (17 matches)
 20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq www (1479 matches)
 30 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 22 (131 matches)
 40 deny icmp any 192.168.60.0 0.0.0.255 echo (2647 matches)
 50 deny tcp any 192.168.60.0 0.0.0.255 eq www (1312 matches)
 60 deny tcp any 192.168.60.0 0.0.0.255 eq 22 (167 matches)
 70 deny ip any any (2410 matches)
router#
```

In the preceding example, access list 150 has dropped the following packets received from an untrusted host or network:

- **2647 ICMP ECHO** packets for ACE line 40
- **1312 HTTP** packets on **TCP port 80 (www)** for ACE line 50
- **167 SSH** packets on **TCP port 22** for ACE line 60

Vulnerabilities Affecting Cisco Unified IP Phones Running SIP Firmware

After the administrator applies the tACL to an interface, the **show ip access-lists** command will identify the number of SIP packets on TCP port 5060 and UDP port 5060, and Telnet packets on TCP port 23 that have been filtered. Administrators are advised to 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 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060 (457 matches)
 20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060 (142 matches)
 30 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq telnet (28 matches)
 40 deny udp any 192.168.60.0 0.0.0.255 eq 5060 (3174 matches)
 50 deny tcp any 192.168.60.0 0.0.0.255 eq 5060 (483 matches)
 60 deny tcp any 192.168.60.0 0.0.0.255 eq telnet (83 matches)
 70 deny ip any any (2145 matches)
router#
```

In the preceding example, access list 150 has dropped the following packets received from an untrusted host or network:

- **3174 SIP** packets on **UDP port 5060** for ACE line 40
- **483 SIP** packets on **TCP port 5060** for ACE line 50
- **83 Telnet** packets on **TCP port 23** for ACE line 60

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.

Embedded Event Manager can be utilized 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 on how to utilize this feature.

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.

For Cisco IOS Software, the **ip access-list logging interval** *interval-in-ms* command can limit the effects of process switching induced by ACL logging. The **logging rate-limit** *rate-per-second* [**except loglevel**] command limits the impact of log generation and transmission.

The CPU impact from ACL logging can be addressed in hardware on the Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers with Supervisor Engine 720 or Supervisor Engine 32 using optimized ACL logging.

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

Identification: Spoofing Protection Using Unicast Reverse Path Forwarding

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

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

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

Note: **show cef interface** *type slot/port internal* is a hidden command that must be fully entered at the command-line interface. Command completion is not available for it.

```
router#show ip interface GigabitEthernet 0/0 | begin verify
--          CLI Output Truncated          --
  IP verify source reachable-via RX, allow default, allow self-ping
  11 verification drops
  0 suppressed verification drops
router#
```

```
router#show cef drop
CEF Drop Statistics
Slot  Encap_fail  Unresolved  Unsupported  No_route  No_adj  ChkSum_Err
RP           27           0           0           18        0        0
router#
```

```
router#show ip traffic
```

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

```

Frag: 0 reassembled, 10008 timeouts, 56866 couldn't reassemble
      0 fragmented, 0 fragments, 0 couldn't fragment
Bcast: 64666 received, 0 sent
Mcast: 1589885 received, 2405454 sent
Sent: 3001564 generated, 65359134 forwarded
Drop: 4256 encapsulation failed, 0 unresolved, 0 no adjacency
      18 no route, 18 unicast RPF, 0 forced drop
      0 options denied
Drop: 0 packets with source IP address zero
Drop: 0 packets with internal loop back IP address
      --      CLI Output Truncated      --
router#

```

In the preceding **show cef drop** and **show ip traffic** examples, Unicast RPF has dropped **18 IP packets** received globally on all interfaces with Unicast RPF configured because of the inability to verify the source address of the IP packets within the Cisco Express 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 with a network attack vector. Administrators are advised to investigate flows to determine whether they are attempts to exploit the vulnerabilities or whether they are legitimate traffic flows.

```

router#show ip cache flow
IP packet size distribution (8270286 total packets):
  1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
    .981 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
    .000 .000 .000 .000 .018 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
 32 active, 4064 inactive, 464 added
8553 aged polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25800 bytes
 0 active, 1024 inactive, 0 added, 0 added to flow
 0 alloc failures, 0 force free
 1 chunk, 1 chunk added
last clearing of statistics never

```

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
TCP-Telnet	10	0.0	11	40	0.0	1.7	15.4
TCP-FTP	5	0.0	8	72	0.0	1.4	6.9
TCP-FTPD	2	0.0	2	175	0.0	0.0	8.4
TCP-WWW	22	0.0	105	40	0.0	0.3	15.3
TCP-other	115	0.0	1312	1492	0.2	0.1	15.3
UDP-other	4	0.0	2028858	28	14.9	20.0	15.5
ICMP	274	0.0	1	77	0.0	2.1	15.4
Total:	432	0.0	19141	54	15.1	1.6	15.3

```

SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP  Pkts
Gi0/1     192.0.2.67        Gi0/0      192.168.60.12     06 0989 0050  30
Gi0/1     192.0.2.36        Gi0/0      192.168.60.52     06 0506 0017  50
Gi0/1     192.0.2.33        Gi0/0      192.168.60.73     06 054A 13C4   1
Gi0/1     192.0.2.37        Gi0/0      192.168.60.11     06 0718 0016 151
Gi0/1     192.0.2.35        Gi0/0      192.168.60.75     06 10E7 0050 121
Gi0/1     192.0.2.31        Gi0/0      192.168.60.17     11 0035 0035   1

```

Gi0/1	192.0.2.58	Gi0/0	192.168.60.18	11	0035	0035	1
Gi0/1	192.0.2.75	Gi0/0	192.168.60.19	11	0035	0035	1
Gi0/1	192.0.2.129	Gi0/0	192.168.60.15	11	0035	0016	6
Gi0/1	192.0.2.91	Gi0/0	192.168.60.14	06	0506	0050	71
Gi0/1	192.168.60.15	Gi0/0	192.168.60.15	01	0000	0800	7
Gi0/1	192.168.60.13	Gi0/0	192.168.60.13	01	0000	0800	1
Gi0/1	192.168.60.11	Gi0/0	192.168.60.11	01	0000	0800	8
Gi0/1	192.168.60.9	Gi0/0	192.168.60.9	01	0000	0800	1

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/1	192.168.60.7	Gi0/0	192.168.60.7	01	0000	0800	43
Gi0/1	192.168.60.5	Gi0/0	192.168.60.5	01	0000	0800	1
Gi0/1	192.168.60.3	Gi0/0	192.168.60.3	01	0000	0800	11
Gi0/1	192.168.60.1	Gi0/0	192.168.60.1	01	0000	0800	1
Gi0/1	192.168.60.14	Gi0/0	192.168.60.14	01	0000	0800	1
Gi0/1	192.168.60.12	Gi0/0	192.168.60.12	01	0000	0800	1
Gi0/1	192.168.60.10	Gi0/0	192.168.60.10	01	0000	0800	76
Gi0/1	192.168.60.8	Gi0/0	192.168.60.8	01	0000	0800	1
Gi0/1	192.168.60.6	Gi0/0	192.168.60.6	01	0000	0800	1
Gi0/1	192.168.60.4	Gi0/0	192.168.60.4	01	0000	0800	156
Gi0/1	192.168.60.2	Gi0/0	192.168.60.2	01	0000	0800	1
Gi0/1	192.0.2.34	Gi0/0	192.168.60.74	06	096C	0016	1
Gi0/1	192.0.2.141	Gi0/0	192.168.60.19	11	0035	00A1	123
Gi0/1	192.0.2.211	Gi0/0	192.168.60.13	06	0718	0050	151
Gi0/1	192.0.2.26	Gi0/0	192.168.60.11	06	16DE	0050	100

router#

In the preceding example, there are multiple flows for **ICMP Echo Request** packets (**Pr = 01, SrcP = 0000, and DstP = 0800**), **SSH** packets on **TCP** port **22** (hex value **0016**), **Telnet** packets on **TCP** port **23** (hex value **0017**), **DNS** packets on **UDP** port **53** (hex value **0035**), **HTTP** packets on **TCP** port **80** (hex value **0050**), and **SIP** packets on **TCP** port **5060** and **UDP** port **5060** (hex value **13C4**). Some of this traffic is sourced from and sent to addresses within the 192.168.60.0/24 address block, which is used by affected devices. The packets in these flows may be spoofed and may indicate an attempt to exploit the vulnerabilities described in this document with a network attack vector. Administrators are advised to compare all flows to baseline utilization and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

To view only the traffic flows for **ICMP Echo Request** packets (**Pr = 01, SrcP = 0000, and DstP = 0800**), **SSH** packets on **TCP** port **22** (hex value **0016**), **Telnet** packets on **TCP** port **23** (hex value **0017**), **DNS** packets on **UDP** port **53** (hex value **0035**), **HTTP** packets on **TCP** port **80** (hex value **0050**), and **SIP** packets on **TCP** port **5060** and **UDP** port **5060** (hex value **13C4**), the command **show ip cache flow | include SrcIf[_11_.*(0035|13C4)]_** will display the related UDP NetFlow records, the command **show ip cache flow | include SrcIf[_06_.*(0016|0017|0035|0050|13C4)]_** will display the related TCP NetFlow records, and the command **show ip cache flow | include SrcIf[_01_.*0800** will display the related ICMP NetFlow records as shown here:

UDP Flows

```
router#show ip cache flow | include SrcIf[_11_.*(0035|13C4)]_
```

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/1	192.0.2.141	Gi0/0	192.168.60.19	11	0035	00A1	123
Gi0/1	192.0.2.38	Gi0/0	192.168.60.3	11	12F4	13C4	15
Gi0/1	192.168.60.10	Gi0/0	192.168.60.10	11	041F	13C4	59
Gi0/1	192.0.2.75	Gi0/0	192.168.60.19	11	0035	0035	1
Gi0/1	192.0.2.129	Gi0/0	192.168.60.15	11	0035	0016	6

router#

TCP Flows

```
router#show ip cache flow | include SrcIf|_06_.*(0016|0017|0035|0050|13C4)_
SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr SrcP DstP  Pkts
Gi0/1     192.0.2.67    Gi0/0     192.168.60.12 06 0989 0050   30
Gi0/1     192.0.2.36    Gi0/0     192.168.60.52 06 0506 0017   50
Gi0/1     192.0.2.33    Gi0/0     192.168.60.73 06 054A 13C4    1
Gi0/1     192.0.2.37    Gi0/0     192.168.60.11 06 0718 0016  151
Gi0/1     192.0.2.35    Gi0/0     192.168.60.75 06 10E7 0050  121
Gi0/1     192.0.2.91    Gi0/0     192.168.60.14 06 0506 0050   71
Gi0/1     192.0.2.34    Gi0/0     192.168.60.74 06 096C 0016    1
Gi0/1     192.0.2.211   Gi0/0     192.168.60.13 06 0718 0050  151
Gi0/1     192.0.2.26    Gi0/0     192.168.60.11 06 16DE 0050  100
router#
```

ICMP Flows

```
router#show ip cache flow | include SrcIf|_01_.*0800
SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr SrcP DstP  Pkts
Gi0/1     192.168.60.15 Gi0/0     192.168.60.15 01 0000 0800    7
Gi0/1     192.168.60.13 Gi0/0     192.168.60.13 01 0000 0800    1
Gi0/1     192.168.60.11 Gi0/0     192.168.60.11 01 0000 0800    8
Gi0/1     192.168.60.9  Gi0/0     192.168.60.9  01 0000 0800    1
Gi0/1     192.168.60.7  Gi0/0     192.168.60.7  01 0000 0800   43
Gi0/1     192.168.60.5  Gi0/0     192.168.60.5  01 0000 0800    1
Gi0/1     192.168.60.3  Gi0/0     192.168.60.3  01 0000 0800   11
Gi0/1     192.168.60.1  Gi0/0     192.168.60.1  01 0000 0800    1
Gi0/1     192.168.60.14 Gi0/0     192.168.60.14 01 0000 0800    1
Gi0/1     192.168.60.12 Gi0/0     192.168.60.12 01 0000 0800    1
Gi0/1     192.168.60.10 Gi0/0     192.168.60.10 01 0000 0800   76
Gi0/1     192.168.60.8  Gi0/0     192.168.60.8  01 0000 0800    1
Gi0/1     192.168.60.6  Gi0/0     192.168.60.6  01 0000 0800    1
Gi0/1     192.168.60.4  Gi0/0     192.168.60.4  01 0000 0800  156
Gi0/1     192.168.60.2  Gi0/0     192.168.60.2  01 0000 0800    1
router#
```

Cisco ASA, PIX, and FWSM Firewalls

Mitigation: Transit Access Control Lists

Vulnerabilities Affecting Cisco Unified IP Phones Running SCCP Firmware

To protect the network from traffic that enters at ingress access points, which may include Internet connection points, partner and supplier connection points, or VPN connection points, administrators are advised to deploy tACLs to perform policy enforcement. Administrators can construct a tACL by explicitly permitting only authorized traffic to enter the network at ingress access points or permitting authorized traffic to transit the network in accordance with existing security policies and configurations. A tACL workaround cannot provide complete protection against the vulnerabilities with a network attack vector when the attack comes from a trusted source address.

The tACL policy denies unauthorized ICMP Echo Requests, HTTP packets on TCP port 80 (www), and SSH packets on TCP port 22 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 available in [Transit Access Control Lists: Filtering at Your Edge](#).

```

!
!-- Include any explicit permit statements for trusted sources
!-- requiring access on the vulnerable ports and protocols
!

access-list Transit-ACL-Policy extended permit icmp host 192.168.100.1 192.168.60.0 255.255
access-list Transit-ACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255
access-list Transit-ACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255

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

access-list Transit-ACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0 echo
access-list Transit-ACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq www
access-list Transit-ACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq ssh

!
!-- 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 interface(s) in the ingress direction
!

access-group Transit-ACL-Policy in interface outside

!

```

Vulnerabilities Affecting Cisco Unified IP Phones Running SIP Firmware

This tACL policy denies unauthorized SIP packets on TCP port 5060 and UDP port 5060 and Telnet packets on TCP port 23 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 available in [Transit Access Control Lists: Filtering at Your Edge](#).

```

!
!-- Include any explicit permit statements for trusted sources
!-- requiring access on the vulnerable ports
!

access-list Transit-ACL-Policy extended permit udp host 192.168.100.1 192.168.60.0 255.255
access-list Transit-ACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255
access-list Transit-ACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255

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

access-list Transit-ACL-Policy extended deny udp any 192.168.60.0 255.255.255.0 eq sip
access-list Transit-ACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq sip
access-list Transit-ACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq telnet

```

```

!
!-- 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 interface(s) in the ingress direction
!

access-group Transit-ACL-Policy in interface outside

!

```

Mitigation: Spoofing Protection Using Unicast Reverse Path Forwarding

Some of the vulnerabilities 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 following vulnerabilities:

Vulnerabilities Affecting Cisco Unified IP Phones Running SCCP Firmware

- Large ICMP Echo Request Denial of Service
- DNS Response Parsing Overflow

Vulnerabilities Affecting Cisco Unified IP Phones Running SIP Firmware

- SIP Proxy Response Overflow
- SIP MIME Boundary Overflow
- DNS Response Parsing Overflow

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

Vulnerabilities Affecting Cisco Unified IP Phones Running SCCP Firmware

After the tACL has been applied to an interface, administrators can use the **show access-list** command to identify the number of ICMP Echo Requests, HTTP packets on TCP port 80 (www), and SSH packets on TCP port 22 that have been filtered. Administrators are advised to 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; 7 elements

```

```

access-list Transit-ACL-Policy line 1 extended permit icmp host 192.168.100.1 192.168.60.0
access-list Transit-ACL-Policy line 2 extended permit tcp host 192.168.100.1 192.168.60.0
access-list Transit-ACL-Policy line 3 extended permit tcp host 192.168.100.1 192.168.60.0
access-list Transit-ACL-Policy line 4 extended deny icmp any 192.168.60.0 255.255.255.0 eq
access-list Transit-ACL-Policy line 5 extended deny tcp any 192.168.60.0 255.255.255.0 eq
access-list Transit-ACL-Policy line 6 extended deny tcp any 192.168.60.0 255.255.255.0 eq
access-list Transit-ACL-Policy line 7 extended deny ip any any (hitcnt=0)
firewall#

```

In the preceding example, access list *Transit-ACL-Policy* has dropped the following packets received from an untrusted host or network:

- **761 ICMP ECHO** packets for ACE line 4
- **98 HTTP** packets on **TCP port 80 (www)** for ACE line 5
- **72 SSH** packets on **TCP port 22** for ACE line 6

Vulnerabilities Affecting Cisco Unified IP Phones Running SIP Firmware

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 TCP port 5060 and UDP port 5060 and Telnet packets on TCP port 23 that have been filtered. Administrators are advised to 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; 7 elements
access-list Transit-ACL-Policy line 1 extended permit udp host 192.168.100.1 192.168.60.0
access-list Transit-ACL-Policy line 2 extended permit tcp host 192.168.100.1 192.168.60.0
access-list Transit-ACL-Policy line 3 extended permit tcp host 192.168.100.1 192.168.60.0
access-list Transit-ACL-Policy line 4 extended deny udp any 192.168.60.0 255.255.255.0 eq
access-list Transit-ACL-Policy line 5 extended deny tcp any 192.168.60.0 255.255.255.0 eq
access-list Transit-ACL-Policy line 6 extended deny tcp any 192.168.60.0 255.255.255.0 eq
access-list Transit-ACL-Policy line 7 extended deny ip any any (hitcnt=0)
firewall#

```

In the preceding example, access list *Transit-ACL-Policy* has dropped the following packets received from an untrusted host or network:

- **412 SIP** packets on **UDP port 5060** for ACE line 4
- **58 SIP** packets on **TCP port 5060** for ACE line 5
- **152 Telnet** packets on **TCP port 23** for ACE line 6

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 potential attempts to exploit the vulnerabilities described in this document with a network attack vector. 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 106023
Dec 19 2007 12:19:58: %ASA-4-106023: Deny udp src outside:192.0.2.39/7136 dst
inside:192.168.60.13/5060 by access-group "Transit-ACL-Policy"
Dec 19 2007 12:19:58: %ASA-4-106023: Deny tcp src outside:192.0.2.39/9451 dst
inside:192.168.60.13/5060 by access-group "Transit-ACL-Policy"
Dec 19 2007 12:04:49: %ASA-4-106023: Deny tcp src outside:192.0.2.39/5854 dst
inside:192.168.60.13/23 by access-group "Transit-ACL-Policy"
Dec 19 2007 12:04:49: %ASA-4-106023: Deny tcp src outside:192.0.2.40/5854 dst
inside:192.168.60.14/23 by access-group "Transit-ACL-Policy"
Dec 19 2007 12:04:49: %ASA-4-106023: Deny tcp src outside:192.0.2.41/5854 dst
inside:192.168.60.15/23 by access-group "Transit-ACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL *Transit-ACL-Policy* show SIP packets on TCP port 5060 and UDP port 5060 and Telnet packets on TCP port 23 sent to the address block assigned to affected devices.

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

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

Identification: Spoofing Protection Using Unicast Reverse Path Forwarding

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

Information about configuring syslog for the Cisco ASA 5500 Series Adaptive Security Appliance or the Cisco PIX 500 Series Security Appliance is available in [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 potential attempts to exploit the vulnerabilities described in this document with a network attack vector. 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
Dec 19 2007 12:26:06: %ASA-1-106021: Deny ICMP reverse path check from
192.168.60.1 to 192.168.60.1 on interface outside
Dec 19 2007 12:24:23: %ASA-1-106021: Deny UDP reverse path check from
192.168.60.140 to 192.168.60.19 on interface outside
Dec 19 2007 12:24:23: %ASA-1-106021: Deny UDP reverse path check from
192.168.60.141 to 192.168.60.20 on interface outside
Dec 19 2007 12:24:23: %ASA-1-106021: Deny UDP reverse path check from
192.168.60.142 to 192.168.60.21 on interface outside
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 debugging accelerated security path dropped packets or connections, reference the Cisco Security Appliance Command Reference for [show asp drop](#).

Cisco Intrusion Prevention System

Mitigation: Cisco IPS Signature Event Actions

Administrators can use the Cisco Intrusion Prevention System (IPS) appliances and services modules to provide threat detection and help prevent attempts to exploit the Large ICMP Echo Request Denial of Service, SIP Proxy Response Overflow vulnerability, and SIP Proxy Response Overflow vulnerabilities described in this document. This vulnerability may be detected by the following signatures:

- 2150 – Fragmented ICMP Traffic
- 2151 – Large ICMP Traffic
- 6781 – SIP Proxy Response Overflow
- 6782 – SIP MIME Request Boundary Overflow

2150 – Fragmented ICMP Traffic

Starting with signature update S2 for sensors running Cisco IPS version 6.x or 5.x, the Large ICMP Echo Request Denial of Service vulnerability can be detected by signature 2150/0 (Signature Name: Fragmented ICMP Traffic). Signature 2150/0 is not enabled by default, triggers an *Informational* severity event, has a signature fidelity rating (SFR) of 100, and is configured with a default event action of **Produce Alert**. Signature 2150/0 fires when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and either the more fragments flag is set to 1 or there is an offset indicated in the offset field. Firing of this signature may indicate a potential exploit of the Large ICMP Echo Request Denial of Service vulnerability.

2151 – Large ICMP Traffic

Starting with signature update S1 for sensors running Cisco IPS version 6.x or 5.x, the Large ICMP Echo Request Denial of Service vulnerability can be detected by signature 2151/0 (Signature Name: Large ICMP Traffic). Signature 2151/0 is not enabled by default, triggers an *Informational* severity event, has an SFR of 100, and is configured with a default event action of **Produce Alert**. Signature 2151/0 fires when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the IP length greater than 1024. Firing of this signature may indicate a potential exploit of the Large ICMP Echo Request Denial of Service vulnerability described in this document.

6781 – SIP Proxy Response Overflow

Starting with signature update S317 for sensors running Cisco IPS version 6.x or 5.x, the SIP Proxy Response Overflow vulnerability described in this document can be detected by signature 6781/0 (Signature Name: SIP Proxy Response Overflow). Signature 6781/0 is enabled by default, triggers a *High* severity event, has an SFR of 85, and is configured with a default event action of **Produce Alert**. Signature 6781/0 fires when a malformed packet is sent by a hostile SIP proxy server. Firing of this signature may indicate a potential exploit of the SIP Proxy Response Overflow vulnerability described in this document.

6782 – SIP MIME Request Boundary Overflow

Starting with signature update S317 for sensors running Cisco IPS version 6.x or 5.x, the SIP MIME Request Boundary Overflow vulnerability described in this document can be detected by signature 6782/0 (Signature Name: SIP MIME Request Boundary Overflow). Signature 6782/0 is enabled by default, triggers a *High* severity event, has an SFR of 85, and is configured with a default event action of **Produce Alert**. Signature 6782/0 fires when a malformed SIP MIME packet that can cause a stack overflow in a SIP client is detected. Firing of this signature may indicate a potential exploit of the SIP MIME Request Boundary Overflow vulnerability 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 Large ICMP Echo Request Denial of Service vulnerability. Due to the potential for false positives, care should be exercised when creating event actions for the Large ICMP Echo Request Denial of Service vulnerability.

Exploits that are easily spoofed may cause a configured event action to inadvertently deny traffic from trusted sources.

Cisco IPS sensors are most effective when deployed in inline protection mode combined with the use of an event action. Automatic Threat Prevention for Cisco IPS 6.x sensors deployed in inline protection mode provides threat prevention against an attack that is attempting to exploit the Large ICMP Echo Request Denial of Service vulnerability. 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: 2150 – Fragmented ICMP Traffic

```
IPS#show events alert
```

```
evIdsAlert: eventId=1184079309279254178 vendor=Cisco severity=informational
originator:
  hostId: R1-IDSM2
  appName: sensorApp
  appInstanceId: 4131
time: February 1, 2008 6:36:32 PM UTC offset=-360 timeZone=CST
signature: description=Fragmented ICMP Traffic id=2150 version=S2
subsigId: 0
```

```
  marsCategory: DoS/Host
interfaceGroup: vs0
vlan: 200
participants:
  attacker:
    addr: 192.168.150.60  locality=OUT
  target:
    addr: 192.168.60.12  locality=OUT
    os:  idSource=unknown  type=unknown  relevance=relevant
```

```
riskRatingValue: 35  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 35
  interface: ge0_0
  protocol: icmp
```

Signature: 2151 – Large ICMP Traffic

IPS#**show events alert**

```
evIdsAlert: eventId=1184079309279254179  vendor=Cisco  severity=informational
originator:
  hostId: R1-IDSM2
  appName: sensorApp
  appInstanceId: 595
time: February 1, 2008 6:36:32 PM UTC  offset=-360  timeZone=CST
signature: description=Large ICMP Traffic  id=2151  version=S1
  subsigId: 0
  marsCategory: DoS/Host
interfaceGroup: vs0
vlan: 200
participants:
  attacker:
    addr: 192.168.150.60  locality=OUT
  target:
    addr: 192.168.60.12  locality=OUT
    os:  idSource=unknown  type=unknown  relevance=relevant
```

```
riskRatingValue: 35  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 35
  interface: ge0_0
  protocol: icmp
```

Signature: 6781 – SIP Proxy Response Overflow

IPS#**show events alert**

```
evIdsAlert: eventId=1197512754360017610  vendor=Cisco  severity=high
originator:
  hostId: R1-IDSM2
  appName: sensorApp
  appInstanceId: 590
time: February 15, 2008 12:12:26 AM UTC  offset=-360  timeZone=CST
signature: description=SIP Proxy Response Overflow  id=6781  version=S317
  subsigId: 0
  sigDetails: SIP Proxy Response Overflow
  marsCategory: Penetrate/BufferOverflow/Misc
interfaceGroup: vs0
vlan: 150
participants:
  attacker:
    addr: 192.168.1.137  locality=OUT
    port: 5060
  target:
```

```
addr: 192.168.1.200 locality=OUT
port: 5060
os: idSource=unknown type=unknown relevance=relevant
```

```
riskRatingValue: 80 targetValueRating=medium attackRelevanceRating=relevant
threatRatingValue: 80
interface: ge0_7
protocol: udp
```

Signature: 6782 – SIP MIME Request Boundary Overflow

```
IPS#show events alert
```

```
evIdsAlert: eventId=1197512754360017612 vendor=Cisco severity=high
originator:
  hostId: R1-IDSM2
  appName: sensorApp
  appInstanceId: 590
time: February 15, 2008 12:12:30 AM UTC offset=-360 timeZone=CST
signature: description=SIP MIME Request Boundary Overflow id=6782 version=S317
  subsigId: 0
  sigDetails: SIP MIME Request Boundary Overflow
  marsCategory: Penetrate/BufferOverflow/Misc
interfaceGroup: vs0
vlan: 150
participants:
  attacker:
    addr: 192.0.2.39 locality=OUT
    port: 32770
  target:
    addr: 192.168.60.15 locality=OUT
    port: 5060
    os: idSource=unknown type=unknown relevance=relevant
```

```
riskRatingValue: 80 targetValueRating=medium attackRelevanceRating=relevant
threatRatingValue: 80
interface: ge0_7
protocol: udp
```

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 on events for the Large ICMP Echo Request Denial of Service vulnerability using IPS signatures 2150/0 (Signature Name: Fragmented ICMP Traffic) and 2151/0 (Signature Name: Large ICMP Traffic). Using keyword **NR-2150/0** for IPS signature 2150/0, **NR-2151/0** for IPS signature 2151/0, and a query type of **All Matching Event Raw Messages** on the Cisco Security MARS appliance will provide a report that lists the incidents created by the IPS signatures.

The following screen shot shows the actual incident created by IPS signatures 2150/0 (Signature Name: Fragmented ICMP Traffic) and 2151/0 (Signature Name: Large ICMP Traffic).

4	ANY	SAFE, STARGETEL, ANY	ANY	Propagate/Copyfiles, Propagate/Worm	ANY	None	ANY	ANY	1)	OR
5	SAFE, STARGETEL, ANY	ANY	icmp (code: ANY, type: ANY, proto: ICMP)	ANY	ANY	None	ANY	ANY	100)	OR
6	SAFE, STARGETEL, ANY	ANY	ANY	Penetrate/GuessPassword/NetworkShares, Penetrate/GuessPassword/WinDomain, Penetrate/GuessPassword/System/Root, Penetrate/GuessPassword/System/Non-root	ANY	None	ANY	ANY	5)	OR

Incident ID: 104033613 Expand All Collapse All

Offset/Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / NIDgate	Tune
5	ICMP Echo Request Trigger packet data	192.168.150.60	192.168.60.12	ICMP	Feb 1, 2008 12:36:29 PM CST	84-IP64346x		Total 2	
5	Fragmented ICMP Traffic Trigger packet data	192.168.150.60	192.168.60.12	ICMP		Groups: 14, Total: 23			
5	Large ICMP Packet Trigger packet data	192.168.150.60	192.168.60.12	ICMP		Groups: 14, Total: 22			
5	Fragmented ICMP Traffic Trigger packet data	192.168.150.60	192.168.60.12	ICMP					
5	Large ICMP Packet Trigger packet data	192.168.150.60	192.168.60.12	ICMP					

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

The following screen shot shows the values used to query for events created by IPS signatures related to the Large ICMP Echo Request Denial of Service vulnerability:

The screenshot shows the Cisco MARS Query Reports interface. The query type is set to "Event Raw Messages ranked by Time, 0h:10m". The query criteria are defined as follows:

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Role	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-2150/0 OR NR-2151/0	None	ANY	ANY

The "Specify raw message keywords:" section shows the following configuration:

Open	Search String	Close	Operation/Highlight
<input type="checkbox"/>	NR-2150/0	<input type="checkbox"/>	OR
<input type="checkbox"/>	NR-2151/0	<input type="checkbox"/>	None

The following screen shot shows the query result for the incidents created by the Cisco Security MARS appliance for the Large ICMP Echo Request Denial of Service vulnerability.

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

Query type: **Event Raw Messages ranked by Time, 0h:10m** [Add] [Clear]

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rate	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-2250/0 OR NR-2152/0	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:32898909, S:32898909	Fragmented ICMP Traffic	Feb 1, 2008 1:17:04 PM CST	R1-IDSM2	192.168.150.60/0 -> 192.168.68.12/0 ICMP Fragmented ICMP Traffic, Rating:35,VLAN:200	Time:1201893454,Risk: [Red]	False Positive Tuning
E:32898920, S:32898920	Large ICMP Packet	Feb 1, 2008 1:17:04 PM CST	R1-IDSM2	192.168.150.60/0 -> 192.168.68.12/0 ICMP Large ICMP Packet, Rating:35,VLAN:200	Time:1201893454,Risk: [Red]	False Positive Tuning
Feb 1, 2008 1:17:34 PM CST	R1-IDSM2	192.168.150.60/0 -> 192.168.68.12/0 ICMP Fragmented ICMP Traffic, Rating:35,VLAN:200		Time:1201893454,Risk: [Red]		False Positive Tuning
Feb 1, 2008 1:17:34 PM CST	R1-IDSM2	192.168.150.60/0 -> 192.168.68.12/0 ICMP Large ICMP Packet, Rating:35,VLAN:200		Time:1201893454,Risk: [Red]		False Positive Tuning
E:32898936, S:32898936	Large ICMP Packet	Feb 1, 2008 1:17:03 PM CST	R1-IDSM2	192.168.150.60/0 -> 192.168.68.12/0 ICMP Large ICMP Packet, Rating:35,VLAN:200	Time:1201893453,Risk: [Red]	False Positive Tuning
E:32898948, S:32898948	Fragmented ICMP Traffic	Feb 1, 2008 1:17:02 PM CST	R4-IPS4240a	192.168.150.60/0 -> 192.168.68.12/0 ICMP Fragmented ICMP Traffic, Rating:35,VLAN:8	Time:1201893452,Risk: [Red]	False Positive Tuning
E:32898959, S:32898959	Large ICMP Packet	Feb 1, 2008 1:17:02 PM CST	R4-IPS4240a	192.168.150.60/0 -> 192.168.68.12/0 ICMP Large ICMP Packet, Rating:35,VLAN:8	Time:1201893452,Risk: [Red]	False Positive Tuning
E:32898970, S:32898970	Fragmented ICMP Traffic	Feb 1, 2008 1:17:02 PM CST	R4-IPS4240a	192.168.150.60/0 -> 192.168.68.12/0 ICMP Fragmented ICMP Traffic, Rating:35,VLAN:8	Time:1201893452,Risk: [Red]	False Positive Tuning
E:32898981, S:32898981	Large ICMP Packet	Feb 1, 2008 1:17:02 PM CST	R4-IPS4240a	192.168.150.60/0 -> 192.168.68.12/0 ICMP Large ICMP Packet, Rating:35,VLAN:8	Time:1201893452,Risk: [Red]	False Positive Tuning
E:32898985, S:32898985	Fragmented ICMP Traffic	Feb 1, 2008 1:17:02 PM CST	R1-IDSM2	192.168.150.60/0 -> 192.168.68.12/0 ICMP Fragmented ICMP Traffic, Rating:35,VLAN:200	Time:1201893452,Risk: [Red]	False Positive Tuning
E:32898976, S:32898976	Large ICMP Packet	Feb 1, 2008 1:17:02 PM CST	R1-IDSM2	192.168.150.60/0 -> 192.168.68.12/0 ICMP Large ICMP Packet, Rating:35,VLAN:200	Time:1201893452,Risk: [Red]	False Positive Tuning
E:32898979, S:32898979	Fragmented ICMP Traffic	Feb 1, 2008 1:17:01 PM CST	R4-IPS4240a	192.168.150.60/0 -> 192.168.68.12/0 ICMP Fragmented ICMP Traffic, Rating:35,VLAN:8	Time:1201893451,Risk: [Red]	False Positive Tuning
E:32898990, S:32898990	Large ICMP Packet	Feb 1, 2008 1:17:01 PM CST	R4-IPS4240a	192.168.150.60/0 -> 192.168.68.12/0 ICMP Large ICMP Packet, Rating:35,VLAN:8	Time:1201893451,Risk: [Red]	False Positive Tuning
E:32898993, S:32898993	Fragmented ICMP Traffic	Feb 1, 2008 1:17:01 PM CST	R4-IPS4240a	192.168.150.60/0 -> 192.168.68.12/0 ICMP Fragmented ICMP Traffic, Rating:35,VLAN:8	Time:1201893451,Risk: [Red]	False Positive Tuning

The Cisco Security MARS appliance can create incidents on events for the SIP Proxy Response Overflow vulnerability using IPS signature 6781/0 (Signature Name: SIP Proxy Response Overflow) and the SIP MIME Boundary Overflow vulnerability using IPS signature 6782/0 (Signature Name: SIP MIME Boundary Overflow). Using keyword **NR-6781/0** for IPS signature 6781/0, **NR-6782/0** for IPS signature 6782/0, and a query type of **All Matching Event Raw Messages** on the Cisco Security MARS appliance will provide a report that lists the incidents created by these IPS signatures.

The following screen shot shows the actual event created by IPS signature 6781/0 (Signature Name: SIP Proxy Response Overflow).

The screenshot displays the Cisco Security MARS interface. At the top, there are navigation tabs: SUMMARY, INCIDENTS, QUERY / REPORTS (selected), RULES, MANAGEMENT, ADMIN, and HELP. Below the tabs, the user is logged in as Administrator (psadmin) and the date is Feb 14, 2008 8:36:06 PM CST. The main content area shows a query report for a specific incident. The incident is titled "Cisco Unified IP Phone SIP Proxy Response Heap Overflow Vulnerability" and is associated with session ID 340011029. The event details table shows the following information:

Event / Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Path / Mitigation	Tune
E:340011029, S:340011029, I:338403478	Cisco Unified IP Phone SIP Proxy Response Heap Overflow Vulnerability	192.168.1.137	192.168.1.200	UDP	Feb 14, 2008 6:12:41 PM CST	R4-IPS4240a		False Positive Tuning

At the bottom of the screen, there is a copyright notice: Copyright © 2003-2007 Cisco Systems, Inc. All rights reserved. The navigation tabs are repeated: Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help.

The following screen shot shows the actual event created by IPS signature 6782/0 (Signature Name: SIP MIME Boundary Overflow).

CISCO SUMMARY INCIDENTS **QUERY / REPORTS** RULES MANAGEMENT ADMIN HELP
 Query Batch Query Report Feb 14, 2008 6:40:44 PM CST
 QUERY / REPORTS | CS-MARS Standalone: R4-MARS v4.3 Login: Administrator (pnadmin) :: Logout :: Activate
 Select Case: No Case Selected... View Cases New Case
 Incident ID: Session ID: 340013311 Show Show
Session Information

Event / Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Path / Mitigation	Tune
E:340013311, S:340013311, I:338403485	Cisco Unified IP Phone SIP Firmware MIME Data Buffer Overflow Vulnerability	192.0.2.39	192.168.60.15	UDP	Feb 14, 2008 6:21:07 PM CST	R1-IDSM2		False Positive Tuning

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

The following screen shot shows the values used to query for events created by IPS signatures 6781/0 and 6782/0.

CISCO SUMMARY INCIDENTS **QUERY / REPORTS** RULES MANAGEMENT ADMIN HELP
 Query Batch Query Report Feb 14, 2008 6:15:20 PM CST
 QUERY / REPORTS | CS-MARS Standalone: R4-MARS v4.3 Login: Administrator (pnadmin) :: Logout :: Activate
 Select Case: No Case Selected... View Cases New Case
Query Event Data
 Click the cells below to change query criteria:
 Query type: Event Raw Messages ranked by Time, 0h:05m Edit Clear

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-6781/0 OR NR-6782/0	None	ANY	ANY

 Apply
 Specify raw message keywords:

Open (Search String) Close	Operation	Highlight
(NR-6781/0)	OR	
(NR-6782/0)	None	
(NR-6781/0)	OR	
(NR-6782/0)	None	
()	None	
()	None	
()	None	
()	None	

The following screen shot shows the query result for the incidents created by the Cisco Security MARS appliance for IPS signatures 6781/0 and 6782/0.

Query type: Event Raw Messages ranked by Time, 0h:05m

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-6781,0 OR NR-6782,0	None	ANY	ANY
E:340011093, S:340011093, I:338403472	Cisco Unified IP Phone SIP Firmware MIME Data Buffer Overflow Vulnerability	Feb 14, 2008	6:12:45 PM CST	R1-IDSM2		192.0.2.39/0 --> 192.168.60.15/0 UDP Cisco Unified IP Phone SIP Firmware MIME Data Buffer Overflow Vulnerability , NR-6782,0,Time:1203034365,Risk Rating:80,VLAN:150,Port List:,0			
E:340011029, S:340011029	Cisco Unified IP Phone SIP Proxy Response Heap Overflow Vulnerability	Feb 14, 2008	6:12:41 PM CST	R4-IPS4240a		192.168.1.137/0 --> 192.168.1.200/0 UDP Cisco Unified IP Phone SIP Proxy Response Heap Overflow Vulnerability , NR-6782,0,Time:1203034361,Risk Rating:80,VLAN:0,Port List:,0			
E:340011093, S:340011093, I:338403472	Cisco Unified IP Phone SIP Firmware MIME Data Buffer Overflow Vulnerability	Feb 14, 2008	6:12:45 PM CST	R1-IDSM2		192.0.2.39/0 --> 192.168.60.15/0 UDP Cisco Unified IP Phone SIP Firmware MIME Data Buffer Overflow Vulnerability , NR-6782,0,Time:1203034365,Risk Rating:80,VLAN:150,Port List:,0			False Positive Tuning
E:340011029, S:340011029	Cisco Unified IP Phone SIP Proxy Response Heap Overflow Vulnerability	Feb 14, 2008	6:12:41 PM CST	R4-IPS4240a		192.168.1.137/0 --> 192.168.1.200/0 UDP Cisco Unified IP Phone SIP Proxy Response Heap Overflow Vulnerability , NR-6782,0,Time:1203034361,Risk Rating:80,VLAN:0,Port List:,0			False Positive Tuning

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, event group mapping, and enable the MARS appliance to parse new signatures from the IPS devices.



Caution: If dynamic signature updates are not configured, events that match these new signatures

appear as unknown event type in queries and reports. MARS will not include these events in inspection rules, thus incidents may not be created for potential threats or attacks that occur within the network.

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

System Rule: CS-MARS IPS Signature Update Failure

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

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

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	2008 – February – 15	Added information for IPS signatures 6781 and 6782.
Revision 1.0	2008 – February – 13	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](#)
- [Protecting Your Core: Infrastructure Protection Access Control Lists](#)
- [Transit Access Control Lists: Filtering at Your Edge](#)
- [Cisco IOS NetFlow – Home Page on Cisco.com](#)
- [Cisco IOS NetFlow White Papers](#)
- [Understanding Access Control List Logging](#)
- [Identifying Incidents Using Firewall and IOS Router Syslog Events](#)
- [Cisco Firewall Products – Home Page on Cisco.com](#)
- [Understanding Unicast Reverse Path Forwarding](#)
- [Unicast Reverse Path Forwarding Loose Mode](#)
- [Unicast Reverse Path Forwarding Enhancements for the Internet Service Provider – Internet Service Provider Network Edge](#)
- [Cisco 6.x Intrusion Prevention System](#)
- [Cisco IPS 6.x Signature Downloads](#)
- [Cisco IPS Signature Search Page](#)
- [Risk Rating and Threat Rating: Simplify IPS Policy Management](#)
- [Cisco Security Monitoring, Analysis, and Response System](#)
- [Cisco Security Center](#)
- [Common Vulnerabilities and Exposures \(CVE\)](#)