

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Remote Access VPN and SIP Vulnerabilities in Cisco PIX and Cisco ASA

<http://www.cisco.com/warp/public/707/cisco-amb-20080903-asa.shtml>

Revision 1.1

Last Updated 2008 September 04 1400 UTC (GMT)

For Public Release 2008 September 03 1600 UTC (GMT)

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

Contents

[Cisco Response](#)
[Device Specific Mitigation and Identification](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)
[Related Information](#)

Cisco Response

This Applied Mitigation Bulletin is a companion document to the PSIRT Security Advisory *Remote Access VPN and SIP Vulnerabilities in Cisco PIX and Cisco ASA* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

There are multiple vulnerabilities in certain releases of PIX and ASA Firewalls. The vulnerabilities are summarized in the following subsections:

Erroneous SIP Processing Vulnerabilities: The vulnerabilities can be exploited remotely without authentication and without user interaction. Successful exploitation of the vulnerabilities may result in a denial of service (DoS) condition. Repeated attempts to exploit the vulnerabilities could result in a sustained DoS condition. The attack vector for exploitation is a specific series of packets destined to TCP port 5060 or UDP port 5060 on the affected device. An attacker could exploit the vulnerabilities using spoofed UDP packets. The vulnerabilities have been assigned CVE identifier CVE-2008-2732. The vulnerabilities are:

- Memory corruption with traceback in SIP inspection code vulnerability.
- Memory corruption and traceback when inspecting malformed SIP packets vulnerability.
- Device reload possible when SIP inspection is enabled vulnerability.
- Traceback when processing malformed SIP requests vulnerability.

IPSec Client Authentication Processing Vulnerability: This vulnerability can be exploited remotely with group authentication and without user interaction. Successful exploitation of this vulnerability may cause the affected device to crash. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through IKE packets using UDP port 500. An attacker could not exploit this vulnerability using spoofed packets. This vulnerability has been assigned CVE identifier CVE-2008-2733.

SSL VPN Memory Leak Vulnerability: This vulnerability can be exploited remotely without authentication and without user interaction. Successful exploitation of this vulnerability may cause the affected device to crash. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through HTTPS packets using TCP port 443. This vulnerability has been assigned CVE identifier CVE-2008-2734.

URI Processing Error Vulnerability in SSL VPNs: This vulnerability can be exploited remotely without authentication and without user interaction. Successful exploitation of this vulnerability may cause the affected device to crash. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through HTTPS packets using TCP port 443. This vulnerability has been assigned CVE identifier CVE-2008-2735.

Potential Information Disclosure in Clientless VPNs: This vulnerability can be exploited remotely without authentication and requires user interaction. Successful exploitation of this vulnerability may allow information disclosure, which enables an attacker to learn information about the affected device. The attack vector for exploitation is through HTTPS packets using TCP port 443. This vulnerability has been assigned CVE identifier CVE-2008-2736.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisory, which is available at the following link: <http://www.cisco.com/warp/public/707/cisco-sa-20080903-asa.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.

For the **Erroneous SIP Processing Vulnerabilities:**

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

- Infrastructure access control lists (iACLs)
- Unicast Reverse Path Forwarding (Unicast RPF)
- IP source guard (IPSG)

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

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

Effective means of exploit prevention can also be provided by 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:

- Transit access control lists (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 that have a network attack vector.

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.

For the **IPSec Client Authentication Processing Vulnerability**, **SSL VPN Memory Leak Vulnerability**, **URI Processing Error Vulnerability in SSL VPNs** and **Potential Information Disclosure in Clientless VPNs** vulnerabilities, Cisco IOS NetFlow can provide visibility into network-based exploitation attempts using flow records.

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: Infrastructure Access Control Lists

To protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, administrators are advised to deploy infrastructure access control lists (iACLs) to perform policy enforcement of traffic sent to infrastructure equipment. Administrators can construct an iACL by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. For the maximum protection of infrastructure devices, deployed iACLs should be applied in the ingress direction on all interfaces to which an IP address has been configured. An iACL workaround cannot provide complete protection against the vulnerabilities that have a network attack vector when the attack comes from a trusted source address.

The iACL policy denies unauthorized SIP packets on TCP port 5060 and UDP port 5060 that are sent to affected devices. In the following example, 192.168.60.0/24 is the IP address space that is used by the affected devices, and the host at 192.168.100.1 is considered a trusted source that requires access to the affected devices. Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic. Whenever possible, infrastructure address space should be distinct from the address space used for user and services segments. Using this addressing methodology will assist with the construction and deployment of iACLs.

Additional information about iACLs is available in [Protecting Your Core: Infrastructure Protection Access Control Lists](#).

```
ip access-list extended Infrastructure-ACL-Policy

!
!-- When applicable, include explicit permit statements for trusted
!-- sources that require access on the vulnerable ports
!

    permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
    permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060

!
!-- The following vulnerability-specific access control entries
```

```

!-- (ACEs) can aid in identification of attacks
!
deny tcp any 192.168.60.0 0.0.0.255 eq 5060
deny udp any 192.168.60.0 0.0.0.255 eq 5060
!
!-- Explicit deny ACE for traffic sent to addresses configured within
!-- the infrastructure address space
!
deny ip any 192.168.60.0 0.0.0.255
!
!-- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations
!
!-- Apply iACL to interfaces in the ingress direction
interface GigabitEthernet0/0
ip access-group Infrastructure-ACL-Policy in
!

```

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

Some of the vulnerabilities described in this document that have a network attack vector 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 **Erroneous SIP Processing Vulnerabilities**.

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

Identification: Infrastructure Access Control Lists

After the administrator applies the iACL to an interface, the **show ip access-lists** command will identify the number of SIP packets on TCP port 5060 and UDP port 5060 that have been filtered on interfaces on which the iACL is applied. Administrators are advised to investigate filtered packets to determine whether they are attempts to exploit the **erroneous SIP processing vulnerabilities**. Example output for **show ip access-lists Infrastructure-ACL-Policy** follows:

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
 10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
 20 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
 30 deny tcp any 192.168.60.0 0.0.0.255 eq 5060 (1531 matches)
 40 deny udp any 192.168.60.0 0.0.0.255 eq 5060 (2051 matches)
 50 deny ip any 192.168.60.0 0.0.0.255
router#
```

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

- **1531 SIP** packets on **TCP port 5060** for ACE line 30
- **2051 SIP** packets on **UDP port 5060** for ACE line 40

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

Administrators can use Embedded Event Manager to provide instrumentation when specific conditions are met, such as ACE counter hits. The Applied Intelligence white paper [Embedded Event Manager in a Security Context](#) provides additional details about how to use this feature.

Identification: Access List Logging

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



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

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

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

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

Identification: Spoofing Protection Using Unicast Reverse Path Forwarding

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

Note: The **show command | begin** *regex* and **show command | include** *regex* command modifiers are used in the following examples to minimize the amount of output that administrators will need to parse to view the desired information. Additional information about command modifiers is 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
<font color="#0000ff">--      CLI Output Truncated      --</font>
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           1             0           0           31        0        0
router#
```

```
router#show ip traffic
```

```
IP statistics:
  Rcvd: 208059135 total, 6480132 local destination
```

```

1150224 format errors, 0 checksum errors, 325905 bad hop count
0 unknown protocol, 38 not a gateway
312 security failures, 4906585 bad options, 5029355 with options
Opts: 32681 end, 29485 nop, 1659 basic security, 8 loose source route
1791 timestamp, 1145 extended security, 741 record route
890 stream ID, 127 strict source route, 67320 alert, 1902 cipso, 0 ump
349644 other
Frag: 0 reassembled, 0 timeouts, 0 couldn't reassemble
0 fragmented, 0 fragments, 0 couldn't fragment
Bcast: 188249 received, 0 sent
Mcast: 4903109 received, 8166939 sent
Sent: 12859414 generated, 196328249 forwarded
Drop: 551838 encapsulation failed, 0 unresolved, 0 no adjacency
31 no route, 31 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 **31 IP packets** received globally on all interfaces with Unicast RPF configured because of the inability to verify the source address of the IP packets within the Cisco Express Forwarding Forwarding Information Base (FIB).

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 that have 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 (171287726 total packets):
  1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
  .000 .435 .087 .014 .042 .025 .016 .004 .010 .001 .002 .002 .002 .005 .007

  512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
  .014 .001 .193 .061 .069 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
19 active, 65517 inactive, 10103716 added
185848843 age polls, 0 flow alloc failures
Active flows timeout in 2 minutes
Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 336520 bytes
0 active, 16384 inactive, 3108973 added, 3108973 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	23067	0.0	27	45	0.1	8.9	30.6
TCP-FTP	955	0.0	8	58	0.0	21.8	22.9

TCP-FTPD	281	0.0	2330	501	0.1	14.7	21.2
TCP-WWW	97381	0.0	13	571	0.3	8.6	34.3
TCP-SMTP	2361	0.0	7	113	0.0	6.7	11.1
TCP-X	5	0.0	1	45	0.0	0.0	60.7
TCP-BGP	1690	0.0	3	44	0.0	13.9	60.6
TCP-NNTP	5	0.0	1	45	0.0	0.0	60.6
TCP-other	7806713	1.8	20	302	36.4	2.0	6.7
UDP-DNS	104227	0.0	4	71	0.1	35.6	44.7
UDP-NTP	586620	0.1	1	76	0.1	4.4	58.7
UDP-TFTP	757	0.0	1	70	0.0	0.4	59.8
UDP-Frag	301039	0.0	6	569	0.4	0.0	15.6
UDP-other	979661	0.2	8	372	1.8	11.3	23.7
ICMP	190411	0.0	5	135	0.2	31.3	48.2
IGMP	10	0.0	2	20	0.0	7.5	60.9
IPINIP	12	0.0	2	20	0.0	1.1	60.8
IPv6INIP	19	0.0	3	75	0.0	0.9	60.9
GRE	4952	0.0	47	52	0.0	119.3	0.9
IP-other	3500	0.0	2	35	0.0	5.4	59.7
Total:	10103666	2.3	16	307	39.8	4.0	13.2

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/0	192.168.208.80	Null	192.168.184.93	06	0D77	0050	3
Gi0/0	192.168.208.80	Null	192.168.184.93	06	0D76	0050	3
Gi0/0	192.168.208.63	Null	192.168.16.89	06	0016	12D1	1
Gi0/0	192.168.208.64	Gi0/1	192.168.150.70	11	E4CD	0035	1
Gi0/0	192.168.208.80	Gi0/1	192.168.150.70	11	0401	0035	4
Gi0/0	192.168.208.64	Gi0/1	192.168.60.44	11	13C5	13C4	1
Gi0/0	192.168.208.64	Gi0/1	192.168.132.44	11	0089	0089	3
Gi0/0	192.168.208.64	Gi0/1	192.168.60.44	11	13C4	13C4	1
Gi0/0	192.168.208.63	Gi0/1	192.168.60.44	06	85CD	13C4	38
Gi0/0	192.168.208.63	Gi0/1	192.168.60.44	06	85CE	13C4	51
Gi0/0	192.168.146.7	Gi0/1	192.168.60.41	06	E621	01BB	6
Gi0/0	192.168.29.211	Gi0/1	192.168.60.41	06	0D8F	01BB	2
Gi0/0	192.168.12.120	Gi0/1	192.168.60.41	11	01F4	01F4	2
Gi0/0	192.168.208.63	Null	192.168.226.1	11	007B	007B	1
Gi0/0	192.168.208.80	Null	192.168.208.255	11	0089	0089	9
Gi0/0	192.168.208.63	Gi0/1	192.168.206.40	01	0000	0303	8

router#

In the preceding example, there are multiple flows for **SIP** packets on **UDP** and **TCP** port **5060** (hex value **13C4**), **IKE** on **UDP** port **500** (hex value **01F4**) and **HTTPS** on **TCP** port **443** (hex value **01BB**). The UDP packets in these flows may be spoofed and may indicate an attempt to exploit the vulnerabilities described in this document that have a network attack vector. Administrators are advised to compare these flows to baseline utilization for SIP traffic sent on UDP and TCP port 5060, HTTPS on TCP 443 and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

Only HTTPS flows that terminate on the IP address of affected ASA and PIX devices can be used to exploit the **IPSec Client Authentication Processing Vulnerability**, **SSL VPN Memory Leak Vulnerability**, **URI Processing Error Vulnerability in SSL VPNs** and **Potential Information Disclosure in Clientless VPNs** vulnerabilities

To view only the traffic flows for **SIP** packets on **TCP** port **5060** and **UDP** port **5060** (hex value **13C4**), **IKE** on **UDP** port **500** (hex value **01F4**) and **HTTPS** on **TCP** port **443** (hex value **01BB**), the command **show ip cache flow | include SrcIf_11.*(13C4|01F4)_** will display the related UDP NetFlow records, the command **show ip cache flow | include SrcIf_06.*(01BB|13C4)_** will display the related TCP

NetFlow records, as shown here:

UDP Flows

```
router#show ip cache flow | include SrcIf|_11_.*(13C4|01F4)_
SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr  SrcP  DstP  Pkts
Gi0/0     192.168.208.64    Gi0/1     192.168.60.44    11  13C4  13C5    1
Gi0/0     192.168.208.64    Gi0/1     192.168.60.44    11  13C4  13C4    1
Gi0/0     192.168.12.120    Gi0/1     192.168.60.41    11  01F4  01F4    2
router#
```

TCP Flows

```
router#show ip cache flow | include SrcIf|_06_.*(01BB|13C4)_
SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr  SrcP  DstP  Pkts
Gi0/0     192.168.208.64    Gi0/1     192.168.60.44    11  13C4  13C4    1
Gi0/0     192.168.208.63    Gi0/1     192.168.60.44    06  85CD  13C4   38
Gi0/0     192.168.208.63    Gi0/1     192.168.60.44    06  85CE  13C4   51
Gi0/0     192.168.146.7     Gi0/1     192.168.60.41    06  E621  01BB    6
Gi0/0     192.168.29.211    Gi0/1     192.168.60.41    06  0D8F  01BB    2
router#
```

Cisco ASA, PIX, and FWSM Firewalls

Mitigation: Transit Access Control Lists

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

The tACL policy denies unauthorized SIP packets on TCP port 5060 and UDP port 5060 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 tcp host 192.168.100.1 192.168.6
access-list Transit-ACL-Policy extended permit udp host 192.168.100.1 192.168.6

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

```

!
access-list Transit-ACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0
access-list Transit-ACL-Policy extended deny udp any 192.168.60.0 255.255.255.0

!
!-- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations
!
!-- Explicit deny for all other IP traffic
!

access-list Transit-ACL-Policy extended deny ip any any

!
!-- Apply tACL to 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 **erroneous SIP processing vulnerabilities**.

Unicast RPF is configured at the interface level and can detect and drop packets that lack a verifiable source IP address. Administrators should not rely on Unicast RPF to provide complete spoofing protection because spoofed packets may enter the network through a Unicast RPF-enabled interface if an appropriate return route to the source IP address exists. In an enterprise environment, Unicast RPF might be enabled at the Internet edge and at the internal access layer on the user-supporting Layer 3 interfaces.

For additional information about the configuration and use of Unicast RPF, reference the Cisco Security Appliance Command Reference for [ip verify reverse-path](#) and the [Understanding Unicast Reverse Path Forwarding](#) Applied Intelligence white paper.

Identification: Transit Access Control Lists

After the tACL has been applied to an interface, administrators can use the **show access-list** command to identify the number of SIP packets on TCP port 5060 and on UDP port 5060 that have been filtered. Administrators are advised to investigate filtered packets to determine whether they are attempts to exploit the **Erroneous SIP Processing Vulnerabilities**. Example output for **show access-list Transit-ACL-Policy** follows:

```

firewall#show access-list Transit-ACL-Policy
access-list Transit-ACL-Policy; 5 elements
access-list Transit-ACL-Policy line 1 extended permit tcp host 192.168.100.1 19
access-list Transit-ACL-Policy line 2 extended permit udp host 192.168.100.1 19
access-list Transit-ACL-Policy line 3 extended deny tcp any 192.168.60.0 255.25
access-list Transit-ACL-Policy line 4 extended deny udp any 192.168.60.0 255.25
access-list Transit-ACL-Policy line 5 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:

- **120 SIP** packets on **TCP port 5060** for ACE line 3
- **140 SIP** packets on **UDP port 5060** for ACE line 4

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 that have 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
Jul 16 2008 17:15:10: %ASA-4-106023: Deny udp src outside:192.168.2.18/2944 dst
    inside:192.168.60.191/5060 by access-group "Transit-ACL-Policy"
Jul 16 2008 17:15:10: %ASA-4-106023: Deny udp src outside:192.168.3.200/2945 ds
    inside:192.168.60.33/5060 by access-group "Transit-ACL-Policy"
firewall#
```

>In the preceding example, the messages logged for the tACL *Transit-ACL-Policy* show potentially spoofed **SIP** packets for **UDP port 5060** 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 that have 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
Jul 16 2008 17:15:21: %ASA-1-106021: Deny UDP reverse path check from
    192.168.0.1 to 192.168.0.100 on interface outside
Jul 16 2008 17:15:21: %ASA-1-106021: Deny UDP reverse path check from
    192.168.0.1 to 192.168.0.100 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 **device reload possible when SIP inspection is enabled vulnerability** described in this document. Starting with signature update S345 for sensors running Cisco IPS version 6.x or 5.x, the **device reload possible when SIP inspection is enabled vulnerability** described in this document can be detected by signature 6520-0 (Signature Name: **Long SIP Message**). Signature 6520-0 is disabled by default, triggers a *Medium* severity event, has a signature fidelity rating (SFR) of 80 and is configured with a default event action of **produce alert**. Signature 6520-0 fires when a single packet sent using UDP port 5060 is detected. Firing of this

signature may indicate a potential exploit of the **device reload possible when SIP inspection is enabled 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 device reload possible when SIP inspection is enabled vulnerability described in this document.

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 device reload possible when SIP inspection is enabled vulnerability described in this document. Threat prevention is achieved through a default override that performs an event action for triggered signatures with a *riskRatingValue* greater than 90.

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

For additional information about the risk rating and threat rating calculation, reference [Risk Rating and Threat Rating: Simplify IPS Policy Management](#).

Identification: IPS Signature Events

Signature:6520-0 Long SIP Message

```
IPS#show events alert
evIdsAlert: eventId=1212721493148127300 severity=medium vendor=Cisco
originator:
  hostId: R4-IPS4240a
  appName: sensorApp
  appInstanceId: 14862
time: 2008/07/24 16:16:24 2008/07/24 11:16:24 CDT
signature: description=Long SIP Message id=6520 version=S345
  subsigId: 0
  sigDetails: Long SIP Message
  marsCategory: Penetrate/BufferOverflow/Misc
interfaceGroup: vs0
vlan: 203
participants:
  attacker:
    addr: locality=OUT 192.168.152.97
    port: 50543
  target:
    addr: locality=OUT 192.168.132.44
    port: 5060
    os: idSource=learned relevance=relevant type=linux
triggerPacket:
```

!-- Packet content removed

```
riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 60
threatRatingValue: 60
interface: ge0_1
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 device reload possible when SIP inspection is enabled vulnerability using IPS signature 6520/0 (Signature Name:Long SIP Message). After the S399 dynamic signature update has been downloaded, using keyword **NR-6520/0** for IPS signature 6520/0 and a query type of **All Matching Events** on the Cisco Security MARS appliance will provide a report that lists the incidents created by the IPS signature.

The following screen shot shows the actual incident created by IPS signature 6520/0 (Signature Name:Long SIP Message):

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

Incidents | False Positives | Cases | Jul 24, 2008 6:32:41 PM CDT

INCIDENTS | CS-MARS Standalone: R4-MARS v4.3 | Login: Administrator (padmin) | Logout | Activate

Select Case: No Case Selected... | View Cases | New Case

Incident ID: Show
 Session ID: Show

Recent Incidents for Last

All Severities | System Rule: Server Attack: Misc. - Attempt | All Case Statuses

Incident ID	Event Type	Matched Rule	Action	Time	Path	Cases
<input type="radio"/> I:370215307	Cisco CallManger Multiple Memory Handling Vulnerabilities	System Rule: Server Attack: Misc. - Attempt		Jul 24, 2008 5:42:01 PM CDT		
<input type="radio"/> I:370215305	Cisco CallManger Multiple Memory Handling Vulnerabilities	System Rule: Server Attack: Misc. - Attempt		Jul 24, 2008 5:51:37 PM CDT		

Event Type	Matched Rule
Cisco CallManger Multiple Memory Handling Vulnerabilities	System Rule: Server Attack: Misc. - Attempt

1 to 6 of 6 | 25 per page

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

The following screen shot shows the value(s) used to query for events created by IPS signatures related to these vulnerabilities:

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

Query Batch Query Report Jul 24, 2008 5:52:05 PM CDT

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

Select Case: No Case Selected... View Cases New Case






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






















Query type: Events ranked by Time, 0d-1h:10m Edit Clear

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-6520/0	None	ANY	ANY

Apply

Specify raw message keywords:

Open (Search String) Close	Operation	Highlight
 	NR-6520/0	 	None	

Search String) Close	Operation
NR-6520/0	 	None
 	 	None
 	 	None
 	 	None
 	 	None
 	 	None

Cancel Apply

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

The following screen shot shows the query results for these vulnerabilities created by the Cisco Security MARS appliance:

Beginning with the 4.3.1 and 5.3.1 releases of Cisco Security MARS appliances, support for the Cisco IPS dynamic signature updates feature has been added. This feature downloads new signatures from Cisco.com or from a local web server, correctly processes and categorizes received events that match those signatures, and includes them in inspection rules and reports. These updates provide event normalization and event group mapping, and they also enable the MARS appliance to parse new signatures from the IPS devices.



Caution: If dynamic signature updates are not configured, events that match these new signatures appear as *unknown event type* in queries and reports. 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, administrators can determine the current signature version downloaded by MARS by selecting **Help > About** and reviewing the *IPS Signature Version* value.

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

Additional Information

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

Revision History

Revision 1.1	2008- September-04	Updated information for Signature pack S345
Revision 1.0	2008- September-03	Initial public release

Cisco Security Procedures

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

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

Related Information

- [Cisco Applied Mitigation Bulletins](#)
- [Cisco Security Center](#)
- [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](#)
- [Cisco Network Foundation Protection White Papers](#)
- [Cisco Network Foundation Protection Presentations](#)
- [Understanding Access Control List Logging](#)
- [Embedded Event Manager in a Security Context](#)
- [Identifying Incidents Using Firewall and IOS Router Syslog Events](#)
- [A Security-Oriented Approach to IP Addressing](#)
- [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](#)
 - [Integrating Cisco Security Agent with Cisco Intrusion Prevention System](#)
 - [Common Vulnerabilities and Exposures \(CVE\)](#)
-

Help us help you.

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Send

[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.](#)