

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco IOS Software Internet Key Exchange Resource Exhaustion Vulnerability

<http://www.cisco.com/warp/public/707/cisco-amb-20090923-ipsec.shtml>

Revision 1.0

For Public Release 2009 September 23 1600 UTC (GMT)

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

Contents

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

Cisco Response

This Applied Mitigation Bulletin is a companion document to the PSIRT Security Advisory *Cisco IOS Software Internet Key Exchange Resource Exhaustion Vulnerability* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

Cisco IOS Software contains an IPSec vulnerability when it processes specially crafted packets. 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 vectors for exploitation are through packets using the following protocols and ports:

- ISAKMP using UDP port 500
- GDOI using UDP port 848
- ISAKMP using UDP port 4500
- GDOI using UDP port 4848

An attacker could exploit this vulnerability using spoofed packets.

This vulnerability has been assigned CVE identifier CVE-2009-2868.

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-20090923-ipsec.shtml>.

Mitigation Technique Overview

Cisco devices provide several countermeasures for this vulnerability. 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:

- 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 this vulnerability.

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

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

Effective exploit prevention can also be provided by the Cisco ASA 5500 Series Adaptive Security Appliance, the Cisco PIX 500 Series Security Appliance, and the Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers using "transit access control lists".

Cisco IOS NetFlow records can provide visibility into network-based exploitation attempts.

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

Risk Management

Organizations are advised to follow their standard risk evaluation and mitigation processes to determine

the potential impact of this vulnerability. Triage refers to sorting projects and prioritizing efforts that are most likely to be successful. Cisco has provided documents that can help organizations develop a risk-based triage capability for their information security teams. [Risk Triage for Security Vulnerability Announcements](#) and [Risk Triage and Prototyping](#) can help organizations develop repeatable security evaluation and response processes.

Device-Specific Mitigation and Identification



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

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

- [Cisco IOS Routers and Switches](#)
- [Cisco IOS NetFlow](#)
- [Cisco ASA, PIX, and FWSM Firewalls](#)

Cisco 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 this vulnerability when the attack originates from a trusted source address.

The iACL policy denies unauthorized ISAKMP packets on UDP port 500 or 4500 and GDOI packets on UDP port 848 or 4848 that are sent to affected devices. In the following example, 192.168.60.0/24 is the IP address space that is used by the affected devices, and the host at 192.168.100.1 is considered a trusted source that requires access to the affected devices. Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic. Whenever possible, infrastructure address space should be distinct from the address space used for user and services segments. Using this addressing methodology will assist with the construction and deployment of iACLs.

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

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

!
!-- Include explicit permit statements for trusted sources
!-- that require access on the vulnerable ports
!
```

```

permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq isakmp
permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 848
permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 4500
permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 4848

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

deny udp any 192.168.60.0 0.0.0.255 eq isakmp
deny udp any 192.168.60.0 0.0.0.255 eq 848
deny udp any 192.168.60.0 0.0.0.255 eq 4500
deny udp any 192.168.60.0 0.0.0.255 eq 4848

!
!-- 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 or 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

The vulnerability that is described in this document can be exploited by spoofed IP packets. Administrators can deploy and configure Unicast Reverse Path Forwarding (Unicast RPF) as a protection mechanism against spoofing.

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

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

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

IP Source Guard

IP source guard (IPSG) is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering packets based on the DHCP snooping binding database and manually configured IP source bindings. Administrators can use IPSG to prevent attacks from an attacker who attempts to spoof packets by forging the source IP address and/or the MAC address. When properly deployed and configured, IPSG coupled with strict mode Unicast RPF provides the most effective means of spoofing protection for the vulnerability that is described in this document.

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

Identification: Infrastructure Access Control Lists

After the administrator applies the iACL to an interface, the **show ip access-lists** command will identify the number of ISAKMP packets on UDP port 500 that have been filtered on interfaces on which the iACL is applied. Administrators should investigate filtered packets to determine whether they are attempts to exploit this vulnerability. Example output for **show ip access-lists Infrastructure-ACL-Policy** follows:

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
 10 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq isakmp
 20 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 848
 30 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 4500
 40 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 4848
 50 deny udp any 192.168.60.0 0.0.0.255 eq isakmp (11 matches)
 60 deny udp any 192.168.60.0 0.0.0.255 eq 848 (14 matches)
 70 deny udp any 192.168.60.0 0.0.0.255 eq 4500 (23 matches)
 80 deny udp any 192.168.60.0 0.0.0.255 eq 4848 (8 matches)
 90 deny ip any 192.168.60.0 0.0.0.255
router#
```

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

- **11 ISAKMP** packets on **UDP port 500** for ACE line 50
- **14 GDOI** packets on **UDP port 848** for ACE line 60
- **23 ISAKMP** packets on **UDP port 4500** for ACE line 70
- **8 GDOI** packets on **UDP port 4848** for ACE line 80

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: Spoofing Protection Using Unicast Reverse Path Forwarding

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

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

```
router#show cef interface GigabitEthernet 0/0 internal | include drop
--          CLI Output Truncated          --
  ip verify: via=rx (allow default), acl=0, drop=18, sdrop=0
router#
```

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

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

```
router#show cef drop
CEF Drop Statistics
Slot  Encap_fail  Unresolved  Unsupported  No_route  No_adj  ChkSum_Err
RP           27           0           0           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 Forwarding Information Base of Cisco Express Forwarding.

Cisco IOS NetFlow

Identification: Traffic Flow Identification Using NetFlow Records

Administrators can configure Cisco IOS NetFlow on Cisco IOS routers and switches to aid in the identification of traffic flows that may be attempts to exploit the vulnerability. Administrators are advised to investigate flows to determine whether they are attempts to exploit the vulnerability or whether they are legitimate traffic flows.

```

router#show ip cache flow
IP packet size distribution (90784136 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000

  512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
  .000 .001 .256 .000 .010 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
1885 active, 63651 inactive, 59960004 added
129803821 ager polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
0 active, 16384 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	11393421	2.8	1	48	3.1	0.0	1.4
TCP-FTP	236	0.0	12	66	0.0	1.8	4.8
TCP-FTPD	21	0.0	13726	1294	0.0	18.4	4.1
TCP-WWW	22282	0.0	21	1020	0.1	4.1	7.3
TCP-X	719	0.0	1	40	0.0	0.0	1.3
TCP-BGP	1	0.0	1	40	0.0	0.0	15.0
TCP-Frag	70399	0.0	1	688	0.0	0.0	22.7
TCP-other	47861004	11.8	1	211	18.9	0.0	1.3
UDP-DNS	582	0.0	4	73	0.0	3.4	15.4
UDP-NTP	287252	0.0	1	76	0.0	0.0	15.5
UDP-other	310347	0.0	2	230	0.1	0.6	15.9
ICMP	11674	0.0	3	61	0.0	19.8	15.5
IPv6INIP	15	0.0	1	1132	0.0	0.0	15.4
GRE	4	0.0	1	48	0.0	0.0	15.3
Total:	59957957	14.8	1	196	22.5	0.0	1.5

```

SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP  Pkts
Gi0/0     192.168.10.201   Gi0/1     192.168.60.102   11 01F4 01F4    1
Gi0/0     192.168.11.54   Gi0/1     192.168.60.158   11 7340 1194    3
Gi0/1     192.168.150.60  Gi0/0     10.89.16.226     06 0016 12CA    1

```

```

Gi0/0      192.168.13.97   Gi0/1      192.168.60.28   11 0350 0350    5
Gi0/0      192.168.10.17   Gi0/1      192.168.60.97   11 01F4 01F4    6
Gi0/0      10.88.226.1     Gi0/1      192.168.202.22  11 007B 007B    1
Gi0/0      192.168.12.185  Gi0/1      192.168.60.239  11 8911 12F0    1
Gi0/0      10.89.16.226    Gi0/1      192.168.150.60  06 12CA 0016    1
router#

```

In the preceding example, there are multiple flows for **ISAKMP** on **UDP port 500 (hex value 01F4)** and port **4500 (hex value 1194)** and **GDOI** on **UDP port 848 (hex value 0350)** and port **484 (hex value 12F0)**.

This traffic is sent to addresses within the 192.168.60.0/24 address block, which is used for infrastructure devices. The packets in these flows may be spoofed and may indicate an attempt to exploit this vulnerability. Administrators are advised to compare these flows to baseline utilization for ISAKMP traffic sent on UDP port 500 and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

To view only the traffic flows for ISAKMP packets on UDP port 500 (hex value 01F4), port 4500 (hex value 1194) port 848 (hex value 0350) and port 4848 (hex value 12F0), the command **show ip cache flow | include SrcIf|_11_.*(01F4|1194|0350|12F0)_** will display the related UDP NetFlow records as shown here:

```

router#show ip cache flow | include SrcIf|_11_.*(01F4|1194|0350|12F0)_
SrcIf      SrcIPAddress    DstIf      DstIPAddress    Pr SrcP DstP  Pkts
Gi0/0      192.168.12.110  Gi0/1      192.168.60.163  11 01F4 01F4    6
Gi0/0      192.168.11.230  Gi0/1      192.168.60.20   11 0350 0350    1
Gi0/0      192.168.11.131  Gi0/1      192.168.60.245  11 01F4 01F4   18
Gi0/0      192.168.13.7    Gi0/1      192.168.60.162  11 01F4 01F4   21
Gi0/0      192.168.11.222  Gi0/1      192.168.60.20   11 8922 12F0    6
Gi0/0      192.168.121.101 Gi0/1      192.168.60.245  11 762E 1194   14
Gi0/0      192.168.183.7   Gi0/1      192.168.60.162  11 89F3 1194   31
Gi0/0      192.168.41.86   Gi0/1      192.168.60.27   11 01F4 01F4    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 this vulnerability when the attack originates from a trusted source address.

The tACL policy denies unauthorized ISAKMP packets on UDP port 500 and port 4500, and GDOI packets on UDP port 848 and port 4848 that are sent to affected devices. In the following example, 192.168.60.0/24 is the IP address space that is used by the affected devices, and the host at 192.168.100.1 is considered a trusted source that requires access to the affected devices. Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic.

Additional information about tACLs is in [Transit Access Control Lists: Filtering at Your Edge](#).

```
!  
!-- Include explicit permit statements for trusted sources  
!-- that require access on the vulnerable ports  
!  
access-list tACL-Policy extended permit udp host 192.168.100.1 192.168.60.0 255  
access-list tACL-Policy extended permit udp host 192.168.100.1 192.168.60.0 255  
access-list tACL-Policy extended permit udp host 192.168.100.1 192.168.60.0 255  
access-list tACL-Policy extended permit udp host 192.168.100.1 192.168.60.0 255  
  
!  
!-- The following vulnerability-specific access control entries  
!-- (ACEs) can aid in identification of attacks  
!  
access-list tACL-Policy extended deny udp any 192.168.60.0 255.255.255.0 eq isa  
access-list tACL-Policy extended deny udp any 192.168.60.0 255.255.255.0 eq 848  
access-list tACL-Policy extended deny udp any 192.168.60.0 255.255.255.0 eq 450  
access-list tACL-Policy extended deny udp any 192.168.60.0 255.255.255.0 eq 484  
  
!  
!-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance  
!-- with existing security policies and configurations  
!  
!-- Explicit deny for all other IP traffic  
!  
access-list tACL-Policy extended deny ip any any  
  
!  
!-- Apply tACL to interface(s) in the ingress direction  
!  
access-group tACL-Policy in interface outside
```

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 ISAKMP packets on UDP port 500 that have been filtered. Administrators are advised to investigate filtered packets to determine whether they are attempts to exploit this vulnerability. Example output for **show access-list tACL-Policy** follows:

```
firewall#show access-list tACL-Policy  
access-list tACL-Policy; 9 elements  
access-list tACL-Policy line 1 extended permit udp host 192.168.100.1 192.168.6  
access-list tACL-Policy line 2 extended permit udp host 192.168.100.1 192.168.6  
access-list tACL-Policy line 3 extended permit udp host 192.168.100.1 192.168.6  
access-list tACL-Policy line 4 extended permit udp host 192.168.100.1 192.168.6  
access-list tACL-Policy line 5 extended deny udp any 192.168.60.0 255.255.255.0  
access-list tACL-Policy line 6 extended deny udp any 192.168.60.0 255.255.255.0  
access-list tACL-Policy line 7 extended deny udp any 192.168.60.0 255.255.255.0  
access-list tACL-Policy line 8 extended deny udp any 192.168.60.0 255.255.255.0  
access-list tACL-Policy line 9 extended deny ip any any (hitcnt=9)  
firewall#
```

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

- **21 ISAKMP** packets on **UDP port 500** for ACE line 5
- **12 GDOI** packets on **UDP port 848** for ACE line 6
- **40 ISAKMP** packets on **UDP port 4500** for ACE line 7
- **17 GDOI** packets on **UDP port 4848** for ACE line 8

Identification: Firewall Access List Syslog Messages

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

Information about configuring syslog for the Cisco ASA 5500 Series Adaptive Security Appliance or the Cisco PIX 500 Series Security Appliance is in [Monitoring the Security Appliance - Configuring and Managing Logs](#). Information about configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is in [Monitoring the Firewall Services Module](#).

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

Additional information about regular expression syntax is in [Creating a Regular Expression](#).

```
firewall#show logging | grep 106023
Jul 23 2009 00:15:13: %ASA-4-106023: Deny udp src outside:192.0.2.18/500
dst inside:192.168.60.191/500 by access-group "tACL-Policy"
Jul 23 2009 00:15:13: %ASA-4-106023: Deny udp src outside:192.2.0.200/500
dst inside:192.168.60.33/500 by access-group "tACL-Policy"
Jul 23 2009 00:15:13: %ASA-4-106023: Deny udp src outside:192.0.2.99/848
dst inside:192.168.60.240/848 by access-group "tACL-Policy"
Jul 23 2009 00:15:13: %ASA-4-106023: Deny udp src outside:192.0.2.100/9676
dst inside:192.168.60.115/4848 by access-group "tACL-Policy"
Jul 23 2009 00:15:13: %ASA-4-106023: Deny udp src outside:192.0.2.88/848
dst inside:192.168.60.38/848 by access-group "tACL-Policy"
Jul 23 2009 00:15:13: %ASA-4-106023: Deny udp src outside:192.0.2.175/5576
dst inside:192.168.60.250/4500 by access-group "tACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL *tACL-Policy* show potentially spoofed **ISAKMP** packets for **UDP port 500** and **port 4500** and **GDOI** packets for **UDP port 848** and **port 4848** sent to the address block assigned to the affected devices.

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

For additional information about investigating incidents using syslog events, reference the [Identifying](#)

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 1.0	2009-SEPTEMBER-23	Initial public release
--------------	-------------------	------------------------

Cisco Security Procedures

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

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

Related Information

- [Cisco Applied Mitigation Bulletins](#)
- [Cisco Guide to Harden Cisco IOS Devices](#)
- [Cisco Security Center](#)
- [Cisco IOS NetFlow - Home Page on Cisco.com](#)
- [Cisco IOS NetFlow White Papers](#)
- [NetFlow Performance Analysis](#)
- [A Security-Oriented Approach to IP Addressing](#)
- [Cisco Firewall Products - Home Page on Cisco.com](#)
- [Unicast Reverse Path Forwarding Enhancements for the Internet Service Provider](#)
- [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](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)