

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Firewall Services Module Crafted ICMP Message Vulnerability

<http://www.cisco.com/warp/public/707/cisco-amb-20090819-fwsm.shtml>

Revision 1.1

Last Updated 2009 September 11 1930 UTC (GMT UTC (GMT)

For Public Release 2009 August 19 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 *Firewall Services Module Crafted ICMP Message Vulnerability* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

The Cisco Firewall Services Module (FWSM) contains a vulnerability when processing specially crafted ICMP packets. This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may cause the affected device to stop forwarding or processing traffic, resulting 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 a specially crafted ICMP packet.

This vulnerability has been assigned CVE identifier CVE-2009-0638.

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-20090819-fwsm.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)
- Transit access control lists (tACLs)

These protection mechanisms filter and drop packets that are attempting to exploit this vulnerability.

Effective exploit prevention can also be provided by the Cisco ASA 5500 Series Adaptive Security Appliance and the Cisco PIX 500 Series Security Appliance using transit access control lists (tACLs). This protection mechanism filters and drops packets that are attempting to exploit this vulnerability.

Effective use of Cisco Intrusion Prevention System (IPS) event actions provides visibility into and protection against attacks that attempt to exploit this vulnerability.

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

Cisco IOS Software, Cisco ASA appliances, and Cisco PIX security appliances 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 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 and PIX 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 this vulnerability when the attack originates from a trusted source address.

The iACL policy denies unauthorized ICMP packet types, including echo request, echo-reply, host-unreachable, traceroute, packet-too-big, time-exceeded, and unreachable, 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 protocol
!

permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 echo
permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 echo-reply
permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 host-unreachable
permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 traceroute
permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 packet-too-big
permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 time-exceeded
```

```

permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 unreachable

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

deny icmp any 192.168.60.0 0.0.0.255 echo
deny icmp any 192.168.60.0 0.0.0.255 echo-reply
deny icmp any 192.168.60.0 0.0.0.255 host-unreachable
deny icmp any 192.168.60.0 0.0.0.255 traceroute
deny icmp any 192.168.60.0 0.0.0.255 packet-too-big
deny icmp any 192.168.60.0 0.0.0.255 time-exceeded
deny icmp any 192.168.60.0 0.0.0.255 unreachable

!
!-- 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 unreachables**. ICMP unreachable rate limiting can be changed from the default using the global configuration command **ip icmp rate-limit unreachable *interval-in-ms***.

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

The tACL policy denies unauthorized ICMP packet types, including echo request, echo-reply, host-unreachable, traceroute, packet-too-big, time-exceeded, and unreachable, 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 protocol
!

access-list 150 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255
echo
access-list 150 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255
echo-reply
access-list 150 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255
host-unreachable
access-list 150 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255
traceroute
access-list 150 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255
packet-too-big
access-list 150 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255
time-exceeded
access-list 150 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255
unreachable

!
!-- 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 icmp any 192.168.60.0 0.0.0.255 echo-reply
access-list 150 deny icmp any 192.168.60.0 0.0.0.255 host-unreachable
access-list 150 deny icmp any 192.168.60.0 0.0.0.255 traceroute
access-list 150 deny icmp any 192.168.60.0 0.0.0.255 packet-too-big
access-list 150 deny icmp any 192.168.60.0 0.0.0.255 time-exceeded
access-list 150 deny icmp any 192.168.60.0 0.0.0.255 unreachable

!
!-- 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 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 unreachables**. ICMP unreachable rate limiting can be changed from the default using the global configuration command **ip icmp rate-limit unreachable interval-in-ms**.

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 ICMP packet types, including echo request, echo-reply, host-unreachable, traceroute, packet-too-big, time-exceeded, and unreachable, 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 icmp host 192.168.100.1 192.168.60.0 0.0.0.255 echo  
 20 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 echo-reply  
 30 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 host-  
unreachable  
 40 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 traceroute  
 50 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 packet-too-  
big  
 60 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 time-  
exceeded  
 70 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 unreachable  
 80 deny icmp any 192.168.60.0 0.0.0.255 echo (34 matches)  
 90 deny icmp any 192.168.60.0 0.0.0.255 echo-reply (25 matches)  
 100 deny icmp any 192.168.60.0 0.0.0.255 host-unreachable (12  
matches)  
 110 deny icmp any 192.168.60.0 0.0.0.255 traceroute (5 matches)  
 120 deny icmp any 192.168.60.0 0.0.0.255 packet-too-big (7 matches)  
 130 deny icmp any 192.168.60.0 0.0.0.255 time-exceeded (20 matches)  
 140 deny icmp any 192.168.60.0 0.0.0.255 unreachable (11 matches)  
 150 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:

- **34 ICMP echo** packets for access control list entry (ACE) line 80
- **25 ICMP echo-reply** packets for ACE line 90
- **12 ICMP host-unreachable** packets for ACE line 100
- **5 ICMP traceroute** packets for ACE line 110

- **7 ICMP packet-too-big** packets for ACE line 120
- **20 ICMP time-exceeded** packets for ACE line 130
- **11 ICMP unreachable** packets for ACE line 140

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: Transit Access Control Lists

After the administrator applies the tACL to an interface, the **show ip access-lists** command will identify the number of ICMP packet types, including echo request, echo-reply, host-unreachable, traceroute, packet-too-big, time-exceeded, and unreachable, 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 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
 20 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 echo-reply
 30 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 host-
unreachable
 40 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 traceroute
 50 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 packet-too-
big
 60 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 time-
exceeded
 70 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 unreachable
 80 deny icmp any 192.168.60.0 0.0.0.255 echo (9 matches)
 90 deny icmp any 192.168.60.0 0.0.0.255 echo-reply (2 matches)
100 deny icmp any 192.168.60.0 0.0.0.255 host-unreachable (18
matches)
110 deny icmp any 192.168.60.0 0.0.0.255 traceroute (3 matches)
120 deny icmp any 192.168.60.0 0.0.0.255 packet-too-big (11 matches)
130 deny icmp any 192.168.60.0 0.0.0.255 time-exceeded (7 matches)
140 deny icmp any 192.168.60.0 0.0.0.255 unreachable (13 matches)
150 deny ip any any
router#
```

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

- **9 ICMP echo** packets for ACE line 80
- **2 ICMP echo-reply** packets for ACE line 90
- **18 ICMP host-unreachable** packets for ACE line 100
- **3 ICMP traceroute** packets for ACE line 110
- **11 ICMP packet-too-big** packets for ACE line 120

- **7 ICMP time-exceeded** packets for ACE line 130
- **13 ICMP unreachable** packets for ACE line 140

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.

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 age 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	Packets	Bytes	Packets	Active(Sec)	
Idle(Sec)	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/
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	01	0984
0800					9
Gi0/0	192.168.11.54	Gi0/1	192.168.60.158	01	0911

```

0000      4
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    01 0B3E
0301    5
Gi0/0    192.168.10.17    Gi0/1    192.168.60.97    01 0B89
0030    1
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    01 0BD7
0200    7
Gi0/0    192.168.15.130  Gi0/1    192.168.60.239    01 0BD7
1100    3
Gi0/0    192.168.23.220  Gi0/1    192.168.60.239    01 0BD7
0300    11
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 the following **ICMP** packet types: **ICMP echo request (hex value 0800)**, **echo-reply (hex value 0000)**, **host-unreachable (hex value 0301)**, **traceroute (hex value 0030)**, **packet-too-big (hex value 0200)**, **time-exceeded (hex value 1100)**, and **unreachable (hex value 0300)**.

To view only the traffic flows for the respective ICMP packet types, the command **show ip cache flow | include SrcIf|_01_.*(0800|0000|0301|0030|0200|1100|0300)_** will display the related ICMP NetFlow records as shown here:

ICMP Flows

```

router#show ip cache flow | include SrcIf|_01_.*(0800|0000|0301|0030|
0200|1100|0300)_
Gi0/0    192.168.10.201    Gi0/1    192.168.60.102    01 0984
0800    9
Gi0/0    192.168.11.54    Gi0/1    192.168.60.158    01 0911
0000    4
Gi0/0    192.168.13.97    Gi0/1    192.168.60.28    01 0B3E
0301    5
Gi0/0    192.168.10.17    Gi0/1    192.168.60.97    01 0B89
0030    1
Gi0/0    192.168.12.185  Gi0/1    192.168.60.239    01 0BD7
0200    7
Gi0/0    192.168.15.130  Gi0/1    192.168.60.239    01 0BD7
1100    3
Gi0/0    192.168.23.220  Gi0/1    192.168.60.239    01 0BD7
0300    11
router#

```

Cisco ASA and PIX 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 ICMP packet types, including echo request, echo-reply, traceroute, packet-too-big, time-exceeded, and unreachable, 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.

Note that in Cisco Firewall ACLs, ICMP "packet-too-big" is specified using the integer "2" which is the designation for ICMP type 2 as seen in the configuration that follows.

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 protocol  
!  
  
access-list tACL-Policy extended permit icmp host 192.168.100.1  
192.168.60.0 255.255.255.0 echo  
access-list tACL-Policy extended permit icmp host 192.168.100.1  
192.168.60.0 255.255.255.0 echo-reply  
access-list tACL-Policy extended permit icmp host 192.168.100.1  
192.168.60.0 255.255.255.0 traceroute  
access-list tACL-Policy extended permit icmp host 192.168.100.1  
192.168.60.0 255.255.255.0 2  
access-list tACL-Policy extended permit icmp host 192.168.100.1  
192.168.60.0 255.255.255.0 time-exceeded  
access-list tACL-Policy extended permit icmp host 192.168.100.1  
192.168.60.0 255.255.255.0 unreachable  
  
!  
!-- The following vulnerability-specific access control entries  
!-- (ACEs) can aid in identification of attacks  
!  
  
access-list tACL-Policy extended deny icmp any 192.168.60.0  
255.255.255.0 echo  
access-list tACL-Policy extended deny icmp any 192.168.60.0  
255.255.255.0 echo-reply  
access-list tACL-Policy extended deny icmp any 192.168.60.0  
255.255.255.0 traceroute  
access-list tACL-Policy extended deny icmp any 192.168.60.0
```

```

255.255.255.0 2
access-list tACL-Policy extended deny icmp any 192.168.60.0
255.255.255.0 time-exceeded
access-list tACL-Policy extended deny icmp any 192.168.60.0
255.255.255.0 unreachable

!
!-- 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 ICMP packet types, such as echo request, echo-reply, traceroute, packet-too-big, time-exceeded, and unreachable, 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; 13 elements
access-list tACL-Policy line 1 extended permit icmp host 192.168.100.1
192.168.60.0 255.255.255.0 echo
access-list tACL-Policy line 2 extended permit icmp host 192.168.100.1
192.168.60.0 255.255.255.0 echo-reply
access-list tACL-Policy line 3 extended permit icmp host 192.168.100.1
192.168.60.0 255.255.255.0 traceroute
access-list tACL-Policy line 4 extended permit icmp host 192.168.100.1
192.168.60.0 255.255.255.0 2
access-list tACL-Policy line 5 extended permit icmp host 192.168.100.1
192.168.60.0 255.255.255.0 time-exceeded
access-list tACL-Policy line 6 extended permit icmp host 192.168.100.1
192.168.60.0 255.255.255.0 unreachable
access-list tACL-Policy line 7 extended deny icmp any 192.168.60.0
255.255.255.0 echo (hitcnt=9)
access-list tACL-Policy line 8 extended deny icmp any 192.168.60.0
255.255.255.0 echo-reply (hitcnt=12)
access-list tACL-Policy line 9 extended deny icmp any 192.168.60.0
255.255.255.0 traceroute (hitcnt=7)
access-list tACL-Policy line 10 extended deny icmp any 192.168.60.0
255.255.255.0 2 (hitcnt=11)

```

```
access-list tACL-Policy line 11 extended deny icmp any 192.168.60.0
255.255.255.0 time-exceeded (hitcnt=5)
access-list tACL-Policy line 12 extended deny icmp any 192.168.60.0
255.255.255.0 unreachable (hitcnt=8)
access-list tACL-Policy line 13 extended deny ip any any (hitcnt=17)
firewall#
```

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

- **9 ICMP echo** packets for ACE line 7
- **12 ICMP echo-reply** packets for ACE line 8
- **7 ICMP traceroute** packets for ACE line 9
- **11 ICMP packet-too-big** packets for ACE line 10
- **5 ICMP time-exceeded** packets for ACE line 11
- **8 ICMP unreachable** packets for ACE line 12

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
  Aug 11 2009 00:15:13: %ASA-4-106023: Deny icmp src
outside:192.0.2.18/2944
      dst inside:192.168.60.191/2048 by access-group "tACL-Policy"
  Aug 11 2009 00:15:13: %ASA-4-106023: Deny icmp src
outside:192.2.0.200/2945
      dst inside:192.168.60.33/0 by access-group "tACL-Policy"
  Aug 11 2009 00:15:13: %ASA-4-106023: Deny icmp src
outside:192.0.2.99/2946
      dst inside:192.168.60.240/48 by access-group "tACL-Policy"
  Aug 11 2009 00:15:13: %ASA-4-106023: Deny icmp src
outside:192.0.2.100/2947
      dst inside:192.168.60.115/512 by access-group "tACL-Policy"
  Aug 11 2009 00:15:13: %ASA-4-106023: Deny icmp src
```

```
outside:192.0.2.88/2949
      dst inside:192.168.60.38/4352  by access-group "tACL-Policy"
Aug 11 2009 00:15:13: %ASA-4-106023: Deny icmp src
outside:192.0.2.175/2950
      dst inside:192.168.60.250/768 by access-group "tACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL *tACL-Policy* show **ICMP** packet types **echo request, echo-reply, traceroute, packet-too-big, time-exceeded, and unreachable** sent to the address block assigned to 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 Incidents Using Firewall and IOS Router Syslog Events](#) Applied Intelligence white paper.

Cisco Intrusion Prevention System

Mitigation: Cisco IPS Signature Event Actions

Administrators can use Cisco Intrusion Prevention System (IPS) appliances and services modules to provide threat detection and help prevent attempts to exploit the vulnerability that is described in this document. Beginning with signature update S426 for sensors running Cisco IPS version 6.x or 5.x, the vulnerability can be detected by signature 20363/0 (Signature Name: Firewall Services Module Crafted ICMP Message Vulnerability). Signature 20363/0 is enabled by default, triggers a *High* severity event, has a signature fidelity rating (SFR) of 95, and is configured with a default event action of **produce-alert**.

Signature 20363/0 fires when a series of crafted ICMP messages are detected. Firing of this signature may indicate a potential exploit of the vulnerability.

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 vulnerability that is described in this document.

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 that are deployed in inline protection mode provides threat prevention against an attack that is attempting to exploit the vulnerability that is 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:](#)

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 regarding events that are related to the vulnerability that is described in this document using IPS signature 20363/0 (Signature Name: Firewall Services Module Crafted ICMP Message Vulnerability). After the S426 dynamic signature update has been downloaded, using keyword **NR-20363/0** for IPS signature 20363/0 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 signature.

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. Because MARS will not include these events in inspection rules, 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 dynamic signature updates and instructions for configuring dynamic signature updates are available 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	2009-September-11	Removed Identification: IPS Signature Events section
Revision 1.0	2009-August-19	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](#)
- [Cisco Network Foundation Protection White Papers](#)
- [Cisco Network Foundation Protection Presentations](#)
- [A Security-Oriented Approach to IP Addressing](#)
- [Securing Tool Command Language on Cisco IOS](#)
- [Cisco Firewall Products - Home Page on Cisco.com](#)
- [Cisco 6.x Intrusion Prevention System](#)
- [Cisco IPS 6.x Signature Downloads](#)
- [Cisco IPS Signature Search Page](#)
- [Cisco Security Monitoring, Analysis, and Response 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)



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.](#)