

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

Applied Mitigation Bulletins

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the CiscoWorks Internetwork Performance Monitor Remote Command Execution Vulnerability

<http://www.cisco.com/warp/public/707/cisco-amb-20080313-ipm.shtml>

Revision 1.0

For Public Release 2008 March 13 1800 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 *CiscoWorks Internetwork Performance Monitor Remote Command Execution Vulnerability* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

CiscoWorks Internet Performance Monitor contains a vulnerability which causes a command shell to be bound to a randomly selected TCP port. This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may allow remote command execution. The attack vector for exploitation is through a TCP connection on a randomly selected TCP port.

This vulnerability has been assigned CVE identifier CVE-2008-1157.

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-20080313-ipm.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 infrastructure access control lists (iACLs). This protection mechanism filters and drops packets that are attempting to exploit this vulnerability.

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 (tACLs). This protection mechanism filters and drops packets that are attempting to exploit this vulnerability.

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.

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 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 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 the vulnerability when the attack comes from a trusted source address.

The iACL policy denies unauthorized TCP packets 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.
!

permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255

!
!-- 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

!
!-- 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**.

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 TCP packets 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 tcp host 192.168.100.1 192.168.60.0 0.0.0.255
 20 deny tcp any 192.168.60.0 0.0.0.255 (6 matches)
 30 deny ip any 192.168.60.0 0.0.0.255
router#
```

In the preceding example, access list *Infrastructure-ACL-Policy* has dropped 6 "packets" for ACE line 20.

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 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 vulnerability when the attack comes from a trusted source address.

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

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

```

!
!-- Include any explicit permit statements for trusted sources
!-- that require access on the vulnerable protocol
!

access-list Transit-ACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 80

!
!-- 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 80

!
!-- 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

!

```

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 TCP packets 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 Transit-ACL-Policy** follows:

```
firewall#show access-list Transit-ACL-Policy
access-list Transit-ACL-Policy; 3 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 deny tcp any 192.168.60.0 255.25
access-list Transit-ACL-Policy line 3 extended deny ip any any (hitcnt=8)
firewall#
```

In the preceding example, access list *Transit-ACL-Policy* has dropped **11 "packets"** of the **TCP protocol** received from an untrusted host or network. In addition, syslog message *106023* can provide valuable information, which includes the source and destination IP address, the source and destination port numbers, and the IP protocol for the denied packet.

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 vulnerability 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 available in [Using the Command Line Interface](#).

```
firewall#show logging | grep 106023
Mar 10 2008 09:24:29: %ASA-4-106023: Deny tcp src outside:192.1.2.6/33526 dst i
Mar 10 2008 09:24:29: %ASA-4-106023: Deny tcp src outside:192.1.2.6/33527 dst i
Mar 10 2008 09:24:29: %ASA-4-106023: Deny tcp src outside:192.1.2.6/33528 dst i
Mar 10 2008 09:24:29: %ASA-4-106023: Deny tcp src outside:192.1.2.6/33529 dst i
firewall#
```

In the preceding example, the messages logged for the tACL *Transit-ACL-Policy* show **TCP** packets sent to the address block assigned to the infrastructure 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.

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	2008-Mar-13	Initial public release
--------------	-------------	------------------------

Cisco Security Procedures

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

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

Related Information

- [Cisco Applied Mitigation Bulletins](#)
- [Protecting Your Core: Infrastructure Protection Access Control Lists](#)
- [Transit Access Control Lists: Filtering at Your Edge](#)
- [Understanding Access Control List Logging](#)
- [Identifying Incidents Using Firewall and IOS Router Syslog Events](#)
- [Cisco Firewall Products - Home Page on Cisco.com](#)
- [Cisco Security Center](#)
- [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](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)