

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

Applied Mitigation Bulletins

# Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Wide Area Application Services (WAAS) Common UNIX Printing System (CUPS) Vulnerability

<http://www.cisco.com/warp/public/707/cisco-amb-20080625-waas.shtml>

## Revision 1.1

Last Updated 2008 August 19 1800 UTC (GMT)

For Public Release 2008 June 25 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 Response *Wide Area Application Services (WAAS) Common UNIX Printing System (CUPS) Vulnerability* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

## Vulnerability Characteristics

The Cisco Wide Area Application Services contains a vulnerability when it processes specially crafted Internet Printing Protocol (IPP) packets. This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may allow arbitrary code execution or result in a denial of service (DoS) condition. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation

is through IPP packets using TCP port 631.

This vulnerability has been assigned CVE identifier CVE-2007-4351.

Vulnerable, non-affected and fixed software information is available in the PSIRT Security Response: <http://www.cisco.com/warp/public/707/cisco-sr-20080625-waas.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 transit access control lists (tACLs). This protection mechanism filters and drops packets that are attempting to exploit the vulnerability that has a network attack vector.

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 the vulnerability that has 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.

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

## Cisco IOS Routers and Switches

### 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 the vulnerability that has a network attack vector when the attack comes from a trusted source address.

The tACL policy denies unauthorized IPP packets on TCP port 631 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 port
!

access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 631

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

access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 631

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

access-list 150 deny ip any any

!
!-- Apply tACL to interfaces in the ingress direction

interface GigabitEthernet0/0
 ip access-group 150 in

!

```

Note that filtering with an interface access list will elicit the transmission of ICMP unreachable messages back to the source of the filtered traffic. Generating these messages could have the undesirable 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: Transit Access Control Lists

After the administrator applies the tACL to an interface, the **show ip access-lists** command will identify the number of IPP packets on TCP port 631 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 tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 631
 20 deny tcp any 192.168.60.0 0.0.0.255 eq 631 (122 matches)
 30 deny ip any any
router#
```

In the preceding example, access list 150 has dropped **122 IPP** packets on **TCP** port **631** 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 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 described in this document that has a network attack vector. 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 (506 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  48
    .324 .673 .000 .000 .001 .000 .000 .000 .000 .000 .000 .000 .000 .000 .00
      512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
      .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  94 active, 4002 inactive, 96 added
  928 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25800 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never

Protocol          Total      Flows      Packets Bytes  Packets Active(Se) Idle(Se)
-----          Flows      /Sec      /Flow  /Pkt  /Sec      /Flow      /Flow
TCP-Telnet             1         0.0         3      60      0.0         8.9        15.6
ICMP                   1         0.0         1     138      0.0         0.0        15.1
Total:                 2         0.0         2      79      0.0         4.4        15.3

SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP  Pk
Et0/0      192.168.46.4      Et0/1      192.168.10.205    06 A607 B586
Et0/0      192.168.236.84   Et0/1      192.168.60.3     06 610F 0277
Et0/0      192.168.126.252  Et0/1      192.168.107.94   06 831E D20C
Et0/0      192.168.205.221  Et0/1      192.168.179.38   11 24F5 98D6
Et0/0      192.168.233.30   Et0/1      192.168.121.133  06 6BAC 3AF4
Et0/0      192.168.125.221  Et0/1      192.168.137.242  11 25C5 174D
Et0/0      192.168.240.172 Et0/1      192.168.60.127   06 C51B 0277
Et0/0      192.168.164.176  Et0/1      192.168.38.20    11 DE48 D9A9
Et0/0      192.168.155.178  Et0/1      192.168.86.254   11 0CBE 1B97
Et0/0      192.168.184.14   Et0/1      192.168.15.182   06 BC0D 06BB
Et0/0      192.168.167.200 Et0/1      192.168.60.73    06 1B1F 0277
Et0/0      192.168.131.158 Et0/1      192.168.60.131   06 7366 0277
Et0/0      192.168.38.164   Et0/1      192.168.54.227   11 D075 8BBD
Et0/0      192.168.129.110 Et0/1      192.168.60.100   06 161E 0277
Et0/0      192.168.241.22   Et0/1      192.168.47.58    11 38CD EEB9
Et0/0      192.168.239.196  Et0/1      192.168.108.177  06 25B9 79FD
Et0/0      192.168.193.100  Et0/1      192.168.251.88   11 58AF BBE9
Et0/0      192.168.37.102   Et0/1      192.168.60.144   06 F8BC 0277
router#
```

In the preceding example, there are multiple flows for IPP on TCP port 631 (hex value 0277). Administrators are advised to compare these flows to baseline utilization for IPP traffic sent on TCP port 631 and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

To view only the traffic flows for IPP packets on TCP port 631 (hex value 0277) use the command **show ip cache flow | include SrcIf\_06\_.\*0277** as shown here:

```
router#show ip cache flow | include SrcIf|_06_.*0277
SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP  Pk
Et0/0      192.168.236.84   Et0/1      192.168.60.3     06 610F 0277
```

```

Et0/0      192.168.240.172 Et0/1      192.168.60.127 06 C51B 0277
Et0/0      192.168.167.200 Et0/1      192.168.60.73  06 1B1F 0277
Et0/0      192.168.131.158 Et0/1      192.168.60.131 06 7366 0277
Et0/0      192.168.129.110 Et0/1      192.168.60.100 06 161E 0277
Et0/0      192.168.37.102  Et0/1      192.168.60.144 06 F8BC 0277
Et0/0      192.168.150.34  Et0/1      192.168.60.50  06 F85E 0277
Et0/0      192.168.74.86   Et0/1      192.168.60.93  06 9B1E 0277
Et0/0      192.168.91.247  Et0/1      192.168.60.58  06 FCB9 0277
Et0/0      192.168.62.97   Et0/1      192.168.60.109 06 5629 0277
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 vulnerability that has a network attack vector when the attack comes from a trusted source address.

The tACL policy denies unauthorized IPP packets on TCP port 631 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 port
!

access-list Transit-ACL-Policy extended permit tcp host 192.168.100.1 192.16

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

access-list Transit-ACL-Policy extended deny tcp any 192.168.60.0 255.255.25

!
!-- 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 IPP packets on TCP port 631 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
access-list Transit-ACL-Policy line 2 extended deny tcp any 192.168.60.0 255
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 **247 IPP** packets on **TCP port 631** received from an untrusted host or network. In addition, syslog message *106023* can provide valuable information, including 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 that has 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
May 14 2008 16:35:31: %ASA-4-106023: Deny tcp src outside:192.168.93.163/575
inside:192.168.60.112/631 by access-group "Transit-ACL-Policy"
May 14 2008 17:18:33: %ASA-4-106023: Deny tcp src outside:192.168.231.104/54
inside:192.168.60.80/631 by access-group "Transit-ACL-Policy"
May 15 2008 08:43:38: %ASA-4-106023: Deny tcp src outside:192.168.64.107/419
inside:192.168.60.165/631 by access-group "Transit-ACL-Policy"
May 15 2008 23:38:00: %ASA-4-106023: Deny tcp src outside:192.168.32.58/2177
inside:192.168.60.85/631 by access-group "Transit-ACL-Policy"
May 16 2008 23:58:54: %ASA-4-106023: Deny tcp src outside:192.168.39.232/220
inside:192.168.60.67/631 by access-group "Transit-ACL-Policy"
```

```

May 17 2008 08:35:56: %ASA-4-106023: Deny tcp src outside:192.168.151.82/408
inside:192.168.60.230/631 by access-group "Transit-ACL-Policy"
May 17 2008 13:46:34: %ASA-4-106023: Deny tcp src outside:192.168.17.169/273
inside:192.168.60.241/631 by access-group "Transit-ACL-Policy"
May 18 2008 02:44:54: %ASA-4-106023: Deny tcp src outside:192.168.61.234/538
inside:192.168.60.214/631 by access-group "Transit-ACL-Policy"
firewall#

```

In the preceding example, the messages logged for the tACL *Transit-ACL-Policy* show **IPP** packets for **TCP port 631** sent to the address block assigned to the infrastructure devices.

## 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- August-19	Corrected link in Vulnerability Overview section
Revision 1.0	2008-June- 25	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](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](#)
- [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](#)
- [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)

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

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