

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

Applied Mitigation Bulletins

# Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco Wireless Control System Tomcat mod\_jk.so Vulnerability

<http://www.cisco.com/warp/public/707/cisco-amb-20080130-wcs.shtml>

## Revision 1.0

For Public Release 2008 January 30 1600 UTC (GMT)

---

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

---

## Contents

- [Cisco Response](#)
- [Device-Specific Mitigation and Identification](#)
- [Cisco IOS Routers and Switches](#)
- [Cisco IOS NetFlow](#)
- [Cisco ASA, PIX, and FWSM Firewalls](#)
- [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 Wireless Control System Tomcat mod\_jk.so Vulnerability* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

## Vulnerability Characteristics

The Cisco Wireless Control System contains a vulnerability when it processes a specially crafted HTTPS packet. This vulnerability can be exploited remotely without authentication and without end-

user interaction. Successful exploitation of this vulnerability may allow arbitrary code execution. The attack vector for exploitation is through HTTPS packets using TCP port 443.

This vulnerability has been assigned CVE identifier CVE-2007-0774.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisory: <http://www.cisco.com/warp/public/707/cisco-sa-20080130-wcs.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 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 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 the vulnerability described in this document. 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.

- [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 described in this document when the attack comes from a trusted source address.

The tACL policy denies unauthorized HTTPS packets on TCP port 443 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 443

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

access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 443

!--- 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 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: Transit Access Control Lists

After the administrator applies the tACL to an interface, the **show ip access-lists** command will identify the number of HTTPS packets on TCP port 443 that have been filtered. Administrators are advised to investigate filtered packets to determine whether they are attempts to exploit the vulnerability described in this document. 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 443
 20 deny tcp any 192.168.60.0 0.0.0.255 eq 443 (422 matches)
 30 deny ip any any
router#
```

In the preceding example, access list 150 has dropped **422 HTTPS** packets on **TCP** port **443** for ACE sequence ID 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, such as ACE counter hits, are met. 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** or **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. 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 (561 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .411 .588 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

  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
  85 active, 4011 inactive, 85 added
  332 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 33992 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(Sec) Idle(Sec)
-----          Flows      /Sec      /Flow  /Pkt   /Sec      /Flow      /Flow

SrcIf            SrcIPAddress  DstIf            DstIPAddress     Pr SrcP DstP  Pkts
Et0/0            192.168.29.209 Et0/1            192.168.14.172   11 0522 8DF3   12
Et0/0            192.168.130.108 Et0/1            192.168.81.234   06 3221 1D76   4
Et0/0            192.168.10.23  Et0/1            192.168.29.191   06 5955 85B0   1
Et0/0            192.168.198.149 Et0/1            192.168.123.124  06 3195 0829   5
Et0/0            192.168.165.220 Et0/1            192.168.60.172   06 C4FA 01BB   14
Et0/0            192.168.226.68 Et0/1            192.168.215.37   11 5F76 E386   3
Et0/0            192.168.10.104 Et0/1            192.168.80.189   06 5E4E C7E9   9
Et0/0            192.168.249.2  Et0/1            192.168.130.113  06 FA8A 7053   2
Et0/0            192.168.116.196 Et0/1            192.168.29.226   11 079E 0B4A   12
Et0/0            192.168.151.166 Et0/1            192.168.113.250  11 5D3A 1AFE   6
Et0/0            192.168.13.35  Et0/1            192.168.179.217  11 CA04 C552   2
Et0/0            192.168.118.37 Et0/1            192.168.95.38    11 E6E8 542B   9
Et0/0            192.168.199.16 Et0/1            192.168.10.59    06 0511 1C32   5
Et0/0            192.168.14.148 Et0/1            192.168.65.221   11 B68D FE87   8
Et0/0            192.168.203.162 Et0/1            192.168.164.103  06 99B0 8E80   7
Et0/0            192.168.18.243 Et0/1            192.168.76.144   06 30AD C0CF   17
Et0/0            192.168.36.197 Et0/1            192.168.44.12    06 C108 EE7A   10
Et0/0            192.168.90.114 Et0/1            192.168.22.181   06 C9C0 8EB0   10
Et0/0            192.168.12.252 Et0/1            192.168.210.212  06 13F2 FACF   5
Et0/0            192.168.252.93 Et0/1            192.168.174.230  11 B422 7692   2
Et0/0            192.168.43.170 Et0/1            192.168.95.102   11 A606 3F6C   3
Et0/0            192.168.160.155 Et0/1            192.168.154.145  11 77DB 3E83   7
Et0/0            192.168.148.91  Et0/1            192.168.60.249   06 22B8 01BB   22
Et0/0            192.168.53.249 Et0/1            192.168.189.76   11 E3D8 CAF9   8
Et0/0            192.168.89.54  Et0/1            192.168.30.14    11 360E 7A5B   3
Et0/0            192.168.26.221 Et0/1            192.168.142.185  06 AD99 604E   1
Et0/0            192.168.198.137 Et0/1            192.168.3.250    11 F505 84D9   7
Et0/0            192.168.251.128 Et0/1            192.168.123.101  11 9931 35A1   13
Et0/0            192.168.139.218 Et0/1            192.168.60.12    06 F1E8 01BB   2
Et0/0            192.168.39.209 Et0/1            192.168.129.131  11 8C91 9E02   6
Et0/0            192.168.112.186 Et0/1            192.168.109.165  06 75E2 277C   4
Et0/0            192.168.202.80 Et0/1            192.168.140.75   06 A46D B1B7   8
router#

```

In the preceding example, there are multiple flows for **HTTPS** on **TCP** port **443** (hex value **01BB**). Administrators are advised to compare these flows to baseline utilization for HTTPS traffic sent on TCP port 443 and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

To view only the traffic flows for HTTPS packets on TCP port 443 (hex value 01BB), use the command **show ip cache flow | include SrcIf|\_06\_.\*01BB** as shown here:

```
router#show ip cache flow | include SrcIf|_06_.*01BB
SrcIf      SrcIPaddress  DstIf      DstIPaddress  Pr SrcP DstP  Pkts
Et0/0     192.168.127.153 Et0/1     192.168.60.187 06 5B84 01BB  3
Et0/0     192.168.109.167 Et0/1     192.168.60.78  06 4D23 01BB  3
Et0/0     192.168.104.202 Et0/1     192.168.60.182 06 2A32 01BB  2
Et0/0     192.168.225.86  Et0/1     192.168.60.197 06 D2DD 01BB  5
Et0/0     192.168.66.78  Et0/1     192.168.60.208 06 39EE 01BB  43
Et0/0     192.168.92.33  Et0/1     192.168.60.21  06 3889 01BB  19
Et0/0     192.168.204.117 Et0/1     192.168.60.149 06 57A0 01BB  1
Et0/0     192.168.94.118  Et0/1     192.168.60.126 06 A73D 01BB  7
Et0/0     192.168.12.35  Et0/1     192.168.60.236 06 3648 01BB  1
Et0/0     192.168.58.208  Et0/1     192.168.60.4   06 151B 01BB  8
Et0/0     192.168.183.157 Et0/1     192.168.60.187 06 5FFA 01BB  7
Et0/0     192.168.40.30  Et0/1     192.168.60.34  06 16B8 01BB  19
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 described in this document when the attack comes from a trusted source address.

The tACL policy denies unauthorized HTTPS packets on TCP port 443 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 Transit-ACL-Policy extended permit tcp host 192.168.100.1 192.168.6

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

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

```
!--- 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 HTTPS packets on TCP port 443 that have been filtered. Administrators are advised to investigate filtered packets to determine whether they are attempts to exploit the vulnerability described in this document. 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=88)
firewall#
```

In the preceding example, access list *Transit-ACL-Policy* has dropped **102 HTTPS** packets on **TCP port 443** 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.

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.

## 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
Dec 18 2007 10:16:02: %ASA-4-106023: Deny tcp src outside:192.168.8.46/19620 ds
  inside:192.168.60.103/443 by access-group "Transit-ACL-Policy"
Dec 18 2007 14:10:07: %ASA-4-106023: Deny tcp src outside:192.168.203.59/49653
  inside:192.168.60.134/443 by access-group "Transit-ACL-Policy"
Dec 19 2007 22:45:39: %ASA-4-106023: Deny tcp src outside:192.168.143.80/49719
  inside:192.168.60.1/443 by access-group "Transit-ACL-Policy"
Dec 20 2007 02:49:51: %ASA-4-106023: Deny tcp src outside:192.168.24.237/53236
  inside:192.168.60.166/443 by access-group "Transit-ACL-Policy"
Dec 20 2007 20:33:10: %ASA-4-106023: Deny tcp src outside:192.168.195.22/61043
  inside:192.168.60.118/443 by access-group "Transit-ACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL *Transit-ACL-Policy* show **HTTPS** packets for **TCP port 443** sent to the address block assigned to affected 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 1.0	2008-January-30	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](#)
- [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](#)
- [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>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 2006-2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).