

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco IOS Software Crafted TCP Sequence and IP Sockets Vulnerabilities

<http://www.cisco.com/warp/public/707/cisco-amb-20090325-tcp-and-ip.shtml>

Revision 1.0

For Public Release 2009 March 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 Advisories *Cisco IOS Software Crafted TCP Sequence Affects SNA, X25 and PPTP Protocol Features* and *Cisco IOS Software Multiple Features IP Sockets Vulnerability* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

There are multiple vulnerabilities in Cisco IOS[®] Software. The following subsections summarize these vulnerabilities:

Cisco IOS Software Crafted TCP Sequence Vulnerability: This vulnerability can be exploited

remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability requires the completion of a three way handshake. Successful exploitation of this vulnerability may cause the affected device to crash. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

The attack vectors for exploitation are through packets using the following protocols and ports:

- Airline Product Set (ALPS) using TCP ports 350 and 10000
- Serial Tunnel Code (STUN) and Block Serial Tunnel Code (BSTUN) using TCP port 1963, ports 1976 through 1979, ports 1990 through 1992 and port 1994
- Native Client Interface Architecture (NCIA) using TCP ports 1981 through 1983, ports 1987 through 1989, port 1996, port 2065 and port 2067
- Data-Link Switching (DLSw) using TCP ports 1981 through 1983, port 2065 and port 2067
- Remote Source-Route Bridging (RSRB) using TCP ports 1987 through 1989 and 1996
- Point to Point Tunneling Protocol (PPTP) using TCP port 1723
- X.25 for Record Boundary Preservation (RBP) using a TCP port defined in the configuration
- X.25 over TCP (XOT) and X.25 Routing using TCP port 1998

This vulnerability has been assigned CVE identifier CVE-2009-0629.

Cisco IOS Software Multiple Features IP Sockets Vulnerability: This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability requires the completion of a three way handshake. Successful exploitation of this vulnerability may cause the affected device to crash. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition.

The attack vectors for exploitation are through packets using the following protocols and ports:

- Cisco Unified Communications Manager Express (Cisco CME) using TCP port 3804
- Session Initiation Protocol (SIP) Gateway Signaling Support using TCP port 2443
- SIP Secure Signaling and Media Encryption using TCP ports 5060 and 5061
- Blocks Extensible Exchange Protocol (BEEP) using a TCP port defined in the configuration
- Various Network Admission Control (NAC) Features using TCP ports 80 and 443
- Distributed Director with HTTP Redirects using TCP ports 53 and 80
- DNS using TCP port 53

This vulnerability has been assigned CVE identifier CVE-2009-0630.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisories, which are available at the following links: <http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml> and <http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml>.

Mitigation Technique Overview

Cisco devices provide several countermeasures for these vulnerabilities. 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).

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).

These protection mechanisms filter and drop packets that are attempting to exploit these vulnerabilities.

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

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

Risk Management

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

Device-Specific Mitigation and Identification

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

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

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

Cisco IOS Routers and Switches

Mitigation: Infrastructure Access Control Lists

To protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, administrators are advised to deploy infrastructure access control lists (iACLs) to perform policy enforcement of traffic sent to infrastructure equipment. Administrators can construct an iACL by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. For the maximum protection of infrastructure devices, deployed iACLs should be applied in the ingress direction on all interfaces to which an IP address has been configured. An iACL workaround cannot provide complete protection against these vulnerabilities when the attack originates from a trusted source address.

The iACL policy denies unauthorized packets sent to affected devices on the following ports:

- ALPS packets on TCP ports 350 and 10000
- STUN packets on TCP ports 1990 through 1992 and port 1994
- BSTUN packets on TCP port 1963 and ports 1976 through 1979
- NCIA packets on TCP ports 1981 through 1983, ports 1987 through 1989, port 1996, port 2065 and port 2067
- DLSw packets on TCP ports 1981 through 1983, port 2065 and port 2067
- RSRB packets on TCP ports 1987 through 1989 and 1996
- PPTP packets on TCP port 1723
- XOT or X.25 Routing packets on TCP port 1998
- Cisco CME packets on TCP port 3804
- SIP Gateway Signaling packets on TCP port 2443
- SIP packets on TCP ports 5060 and 5061
- HTTP packets on TCP port 80
- HTTPS packets on TCP port 443
- DNS packets on TCP port 53

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

!
!-- When applicable, include explicit permit statements for trusted
!-- sources that require access on the vulnerable ports
!

permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 350
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 10000
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 range 1990 1992
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1994
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1963
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 range 1976 1979
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 range 1981 1983
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 range 1987 1989
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1996
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 2065
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 2067
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1723
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1998
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 3804
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 2443
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 range 5060 5061
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 80
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 53

!
!-- 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 eq 350
deny tcp any 192.168.60.0 0.0.0.255 eq 10000
deny tcp any 192.168.60.0 0.0.0.255 range 1990 1992
deny tcp any 192.168.60.0 0.0.0.255 eq 1994
deny tcp any 192.168.60.0 0.0.0.255 eq 1963
deny tcp any 192.168.60.0 0.0.0.255 range 1976 1979
deny tcp any 192.168.60.0 0.0.0.255 range 1981 1983
deny tcp any 192.168.60.0 0.0.0.255 range 1987 1989
deny tcp any 192.168.60.0 0.0.0.255 eq 1996
deny tcp any 192.168.60.0 0.0.0.255 eq 2065
deny tcp any 192.168.60.0 0.0.0.255 eq 2067
deny tcp any 192.168.60.0 0.0.0.255 eq 1723
deny tcp any 192.168.60.0 0.0.0.255 eq 1998
deny tcp any 192.168.60.0 0.0.0.255 eq 3804
deny tcp any 192.168.60.0 0.0.0.255 eq 2443
deny tcp any 192.168.60.0 0.0.0.255 range 5060 5061
deny tcp any 192.168.60.0 0.0.0.255 eq 80
deny tcp any 192.168.60.0 0.0.0.255 eq 443
deny tcp any 192.168.60.0 0.0.0.255 eq 53

!
!-- 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 packets of the following protocols that have been filtered on interfaces on which the iACL is applied:

- ALPS packets on TCP ports 350 and 10000
- STUN packets on TCP ports 1990 through 1992 and port 1994

- BSTUN packets on TCP port 1963 and ports 1976 through 1979
- NCIA packets on TCP ports 1981 through 1983, ports 1987 through 1989, port 1996, port 2065 and port 2067
- DLSw packets on TCP ports 1981 through 1983, port 2065 and port 2067
- RSRB packets on TCP ports 1987 through 1989 and 1996
- PPTP packets on TCP port 1723
- XOT or X.25 Routing packets on TCP port 1998
- Cisco CME packets on TCP port 3804
- SIP Gateway Signaling packets on TCP port 2443
- SIP packets on TCP ports 5060 and 5061
- HTTP packets on TCP port 80
- HTTPS packets on TCP port 443
- DNS packets on TCP port 53

Administrators should investigate filtered packets to determine whether they are attempts to exploit these vulnerabilities. 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 eq 350
 20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 10000
 30 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 range 1990 1992
 40 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1994
 50 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1963
 60 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 range 1976 1979
 70 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 range 1981 1983
 80 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 range 1987 1989
 90 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1996
100 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 2065
110 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 2067
120 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1723
130 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1998
140 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 3804
150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 2443
160 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 range 5060 5061
170 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq www
180 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
190 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq domain
200 deny tcp any 192.168.60.0 0.0.0.255 eq 350 ( 4 matches)
210 deny tcp any 192.168.60.0 0.0.0.255 eq 10000 ( 7 matches)
220 deny tcp any 192.168.60.0 0.0.0.255 range 1990 1992 ( 16 matches)
230 deny tcp any 192.168.60.0 0.0.0.255 eq 1994 ( 9 matches)
240 deny tcp any 192.168.60.0 0.0.0.255 eq 1963 ( 2 matches)
250 deny tcp any 192.168.60.0 0.0.0.255 range 1976 1979 ( 8 matches)
260 deny tcp any 192.168.60.0 0.0.0.255 range 1981 1983 ( 24 matches)
270 deny tcp any 192.168.60.0 0.0.0.255 range 1987 1989 ( 34 matches)
280 deny tcp any 192.168.60.0 0.0.0.255 eq 1996 ( 11 matches)
290 deny tcp any 192.168.60.0 0.0.0.255 eq 2065 ( 6 matches)
300 deny tcp any 192.168.60.0 0.0.0.255 eq 2067 ( 3 matches)
310 deny tcp any 192.168.60.0 0.0.0.255 eq 1723 ( 3 matches)
320 deny tcp any 192.168.60.0 0.0.0.255 eq 1998 ( 12 matches)
330 deny tcp any 192.168.60.0 0.0.0.255 eq 3804 ( 7 matches)
340 deny tcp any 192.168.60.0 0.0.0.255 eq 2443 ( 5 matches)
350 deny tcp any 192.168.60.0 0.0.0.255 range 5060 5061 ( 41 matches)
360 deny tcp any 192.168.60.0 0.0.0.255 eq www ( 56 matches)
370 deny tcp any 192.168.60.0 0.0.0.255 eq 443 ( 20 matches)
380 deny tcp any 192.168.60.0 0.0.0.255 eq domain ( 4 matches)
```

```
390 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:

- **4 ALPS** packets on **TCP port 350** for ACE line 200
- **7 ALPS** packets on **TCP port 10000** for ACE line 210
- **16 STUN** packets on **TCP ports 1990 through 1992** for ACE line 220
- **9 STUN** packets on **TCP port 1994** for ACE line 230
- **2 BSTUN** packets on **TCP port 1963** for ACE line 240
- **8 BSTUN** packets on **TCP ports 1976 through 1979** for ACE line 250
- **24 NCIA or DLSw** packets on **TCP ports 1981 through 1983** for ACE line 260
- **34 NCIA or RSRB** packets on **TCP ports 1987 through 1989** for ACE line 270
- **11 NCIA or RSRB** packets on **TCP port 1996** for ACE line 280
- **6 NCIA or DLSw** packets on **TCP port 2065** for ACE line 290
- **3 NCIA or DLSw** packets on **TCP port 2067** for ACE line 300
- **3 PPTP** packets on **TCP port 1723** for ACE line 310
- **12 XOT or X.25 Routing** packets on **TCP port 1998** for ACE line 320
- **7 CUCME** packets on **TCP port 3804** for ACE line 330
- **5 SIP Gateway Signaling** packets on **TCP port 2443** for ACE line 340
- **41 SIP** packets on **TCP ports 5060 and 5061** for ACE line 350
- **56 HTTP** packets on **TCP port 80** for ACE line 360
- **20 HTTPS** packets on **TCP port 443** for ACE line 370
- **4 DNS** packets on **TCP port 53** for ACE line 380

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 these vulnerabilities. Administrators are advised to investigate flows to determine whether they are attempts to exploit these vulnerabilities or whether they are legitimate traffic flows.

```

router# show ip cache flow
IP packet size distribution (87473091 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .000 .370 .240 .084 .072 .016 .046 .018 .001 .000 .007 .002 .000 .000 .001

      512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
      .001 .000 .032 .022 .079 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  20 active, 65516 inactive, 9809179 added
  347876063 ager polls, 0 flow alloc failures
  Active flows timeout in 2 minutes
  Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 533256 bytes
  20 active, 16364 inactive, 9809179 added, 9809179 added to flow
  0 alloc failures, 2161 force free
  1 chunk, 6 chunks added
  last clearing of statistics never

```

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
TCP-Telnet	10133	0.0	8	43	0.0	2.2	24.5
TCP-FTP	6940	0.0	2	51	0.0	0.8	48.0
TCP-FTPD	2974	0.0	72	736	0.0	0.3	46.9
TCP-WWW	160068	0.0	37	729	1.5	25.9	17.1
TCP-SMTP	4169	0.0	1	73	0.0	10.7	45.7
TCP-X	2853	0.0	1	43	0.0	0.0	50.6
TCP-BGP	2761	0.0	1	43	0.0	0.0	50.1
TCP-NNTP	2771	0.0	1	43	0.0	0.0	49.8
TCP-Frag	2	0.0	105	1436	0.0	17.0	60.2
TCP-other	7049380	1.7	6	235	11.3	1.1	28.8
UDP-DNS	148727	0.0	4	66	0.1	21.1	50.6
UDP-NTP	215800	0.0	1	76	0.0	5.7	58.3
UDP-TFTP	4	0.0	1	28	0.0	0.0	60.3
UDP-other	926078	0.2	31	124	7.4	19.8	52.3
ICMP	857726	0.2	2	75	0.4	3.8	59.9
IGMP	132997	0.0	2	39	0.0	58.9	42.3
IPINIP	4	0.0	16	137	0.0	84.8	26.5
IPv6INIP	5	0.0	12	143	0.0	69.7	31.8
GRE	466	0.0	1	20	0.0	0.2	60.4
IP-other	285301	0.0	10	95	0.7	91.9	16.6
Total:	9809159	2.4	8	222	21.9	7.3	34.4

```

SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP  Pkts
Gi0/0     10.21.64.147     Gi0/1     192.168.128.21   06 0770 07BD   1
Gi0/0     192.168.208.49  Gi0/1     255.255.255.255  11 0044 0043   3

```

Gi0/0	192.168.208.127	Gi0/0	172.18.104.132	06	BD40	13C4	7
Gi0/0	172.18.104.132	Gi0/1	192.168.150.60	06	1A29	0EDC	1
Gi0/0	192.168.208.111	Null	255.255.255.255	11	1375	2FBF	5
Gi0/0	10.98.29.213	Gi0/1	192.168.130.41	06	0E13	13C5	6
Gi0/0	10.88.226.1	Gi0/1	192.168.144.3	11	007B	007B	1
Gi0/0	10.89.17.226	Local	192.168.128.20	06	E348	0035	129
Gi0/0	10.88.226.1	Local	192.168.128.20	11	007B	007B	1
Gi0/0	10.101.128.56	Gi0/1	192.168.132.44	06	0035	0050	8
Gi0/0	10.21.88.103	Gi0/1	192.168.130.41	06	EB24	098B	6

router#

In the preceding example, there are multiple flows for **TCP** ports **1981 through 1983** (hex value **07BD through 07BF**), **CAPF** on **TCP** port **3804** (hex value **0EDC**), **TCP** port **2443** (hex value **098B**), **SIP** on **TCP** ports **5060 and 5061** (hex value **13C4 and 13C5**), **HTTP** on **TCP** port **80** (hex value **0050**) and **DNS** on **TCP** port **53** (hex value **0035**).

To view only specific traffic flows for a single protocol, one of the following commands may be used:

For ALPS packets on TCP ports 350 and 10000 (hex value 015E and 2710), the command **show ip cache flow | include SrcIf|_06_|*(015E|2710)_** will display only ALPS related TCP packets.

For STUN packets on TCP ports 1990 through 1992 and port 1994 (hex values 07C6 through 07C8 and 07CA) the command **show ip cache flow | include SrcIf|_06_|*(07C6|07C7|07C8|07CA)_** will display only STUN related TCP packets.

For BSTUN packets on TCP port 1963 and ports 1976 through 1979 (hex values 07AB and 07B8 through 07BB) the command **show ip cache flow | include SrcIf|_06_|*(07AB|07B8|07B9|07BA|07BB)_** will display only BSTUN related TCP packets.

For NCIA packets on TCP ports 1981 through 1983, ports 1987 through 1989, port 1996, port 2065 and port 2067 (hex values 07BD through 07BF, 07C3 through 07C5, 07CC, 0811 and 0813) the command **show ip cache flow | include SrcIf|_06_|*(07BD|07BE|07BF|07C3|07C4|07C5|07CC|0811|0813)_** will display only NCIA related TCP packets.

For DLSw packets on TCP ports 1981 through 1983, port 2065 and port 2067 (hex values 07BD through 07BF, 0811 and 0813) the command **show ip cache flow | include SrcIf|_06_|*(07BD|07BE|07BF|0811|0813)_** will display only DLSw related TCP packets.

For RSRB packets on TCP ports 1987 through 1989 and 1996 (hex values 07C3 through 07C5 and 07CC) the command **show ip cache flow | include SrcIf|_06_|*(07C3|07C4|07C5|07CC)_** will display only RSRB related TCP packets.

For PPTP packets on TCP port 1723 (hex value 06BB) the command **show ip cache flow | include SrcIf|_06_|*(06BB)_** will display only PPTP related TCP packets.

For XOT or X.25 Routing packets on TCP port 1998 (hex value 07CE) the command **show ip cache flow | include SrcIf|_06_|*(07CE)_** will display only XOT or X.25 Routing related TCP packets.

For Cisco CME packets on TCP port 3804 (hex value 0EDC) the command **show ip cache flow | include SrcIf|_06_|*(0EDC)_** will display only Cisco CME related TCP packets.

For SIP Gateway Signaling packets on TCP port 2443 (hex value 098B) the command **show ip cache**

flow | include SrcIf|_06_.*(098B)_ will display only SIP Gateway related TCP packets.

For SIP packets on TCP ports 5060 and 5061 (hex value 13C4 and 13C5) the command **show ip cache flow | include SrcIf|_06_.*(13C4|13C5)_** will display only SIP related TCP packets.

For HTTP packets on TCP port 80 and HTTPS packets on port 443 (hex values 0050 and 01BB) the command **show ip cache flow | include SrcIf|_06_.*(0050|01BB)_** will display only HTTP and HTTPS related TCP packets.

For HTTP packets on TCP port 80 and DNS packets on TCP port 53 (hex values 0050 and 0035) the command **show ip cache flow | include SrcIf|_06_.*(0050|0035)_** will display only HTTP and DNS related TCP packets.

Sample output for DLSw related TCP packets with the command **show ip cache flow | include SrcIf|_06_.*(07BD|07BE|07BF|0811|0813)_** is shown here:

```
router# show ip cache flow | include SrcIf|_06_.*(07BD|07BE|07BF|0811|0813)_
SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr  SrcP  DstP  Pkts
Gi0/0     192.168.12.110    Gi0/1     192.168.60.163    06 092A 07BD    6
Gi0/0     192.168.11.230   Gi0/1     192.168.60.20    06 0C09 0811    1
Gi0/0     192.168.11.131   Gi0/1     192.168.60.245   06 0B66 07BD   18
Gi0/0     192.168.13.7     Gi0/1     192.168.60.162   06 0914 07BE    1
Gi0/0     192.168.41.86    Gi0/1     192.168.60.27    06 0B7B 0813    2
Gi0/0     192.168.143.7    Gi0/1     192.168.60.102   06 0914 07BF    1
Gi0/0     192.168.141.27   Gi0/1     192.168.60.47    06 0B7B 0811    2
router#
```

Cisco ASA, PIX, and FWSM Firewalls

Mitigation: Transit Access Control Lists

To protect the network from traffic that enters the network at ingress access points, which may include Internet connection points, partner and supplier connection points, or VPN connection points, administrators are advised to deploy tACLs to perform policy enforcement. Administrators can construct a tACL by explicitly permitting only authorized traffic to enter the network at ingress access points or permitting authorized traffic to transit the network in accordance with existing security policies and configurations. A tACL workaround cannot provide complete protection against these vulnerabilities when the attack originates from a trusted source address.

The tACL policy denies unauthorized packets of the following protocols that are sent to affected devices:

- ALPS packets on TCP ports 350 and 10000
- STUN packets on TCP ports 1990 through 1992 and port 1994
- BSTUN packets on TCP port 1963 and ports 1976 through 1979
- NCIA packets on TCP ports 1981 through 1983, ports 1987 through 1989, port 1996, port 2065 and port 2067
- DLSw packets on TCP ports 1981 through 1983, port 2065 and port 2067
- RSRB packets on TCP ports 1987 through 1989 and 1996
- PPTP packets on TCP port 1723
- XOT or X.25 Routing packets on TCP port 1998
- Cisco CME packets on TCP port 3804


```

access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 380
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 244
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 range
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 80
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 443
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 53

!
!-- 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 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 packets of the following protocols that have been filtered:

- ALPS packets on TCP ports 350 and 10000
- STUN packets on TCP ports 1990 through 1992 and port 1994
- BSTUN packets on TCP port 1963 and ports 1976 through 1979
- NCIA packets on TCP ports 1981 through 1983, ports 1987 through 1989, port 1996, port 2065 and port 2067
- DLSw packets on TCP ports 1981 through 1983, port 2065 and port 2067
- RSRB packets on TCP ports 1987 through 1989 and 1996
- PPTP packets on TCP port 1723
- XOT or X.25 Routing packets on TCP port 1998
- Cisco CME packets on TCP port 3804
- SIP Gateway Signaling packets on TCP port 2443
- SIP packets on TCP ports 5060 and 5061
- HTTP packets on TCP port 80
- HTTPS packets on TCP port 443
- DNS packets on TCP port 53

Administrators are advised to investigate filtered packets to determine whether they are attempts to exploit these vulnerabilities. Example output for **show access-list tACL-Policy** follows:

```

firewall# show access-list tACL-Policy
access-list tACL-Policy; 39 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1 192.168.6
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1 192.168.6
access-list tACL-Policy line 3 extended permit tcp host 192.168.100.1 192.168.6
access-list tACL-Policy line 4 extended permit tcp host 192.168.100.1 192.168.6
access-list tACL-Policy line 5 extended permit tcp host 192.168.100.1 192.168.6
access-list tACL-Policy line 6 extended permit tcp host 192.168.100.1 192.168.6
access-list tACL-Policy line 7 extended permit tcp host 192.168.100.1 192.168.6

```

```

access-list tACL-Policy line 8 extended permit tcp host 192.168.100.1 192.168.6
access-list tACL-Policy line 9 extended permit tcp host 192.168.100.1 192.168.6
access-list tACL-Policy line 10 extended permit tcp host 192.168.100.1 192.168.
access-list tACL-Policy line 11 extended permit tcp host 192.168.100.1 192.168.
access-list tACL-Policy line 12 extended permit tcp host 192.168.100.1 192.168.
access-list tACL-Policy line 13 extended permit tcp host 192.168.100.1 192.168.
access-list tACL-Policy line 14 extended permit tcp host 192.168.100.1 192.168.
access-list tACL-Policy line 15 extended permit tcp host 192.168.100.1 192.168.
access-list tACL-Policy line 16 extended permit tcp host 192.168.100.1 192.168.
access-list tACL-Policy line 17 extended permit tcp host 192.168.100.1 192.168.
access-list tACL-Policy line 18 extended permit tcp host 192.168.100.1 192.168.
access-list tACL-Policy line 19 extended permit tcp host 192.168.100.1 192.168.
access-list tACL-Policy line 20 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 21 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 22 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 23 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 24 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 25 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 26 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 27 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 28 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 29 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 30 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 31 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 32 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 33 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 34 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 35 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 36 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 37 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 38 extended deny tcp any 192.168.60.0 255.255.255.
access-list tACL-Policy line 39 extended deny ip any any

```

```
firewall#
```

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

- **5 ALPS** packets on **TCP port 350** for ACE line 20
- **2 ALPS** packets on **TCP port 10000** for ACE line 21
- **6 STUN** packets on **TCP ports 1990 through 1992** for ACE line 22
- **12 STUN** packets on **TCP port 1994** for ACE line 23
- **6 BSTUN** packets on **TCP port 1963** for ACE line 24
- **14 BSTUN** packets on **TCP ports 1976 through 1979** for ACE line 25
- **18 NCIA or DLSw** packets on **TCP ports 1981 through 1983** for ACE line 26
- **3 NCIA or RSRB** packets on **TCP ports 1987 through 1989** for ACE line 27
- **9 NCIA or RSRB** packets on **TCP port 1996** for ACE line 28
- **7 NCIA or DLSw** packets on **TCP port 2065** for ACE line 29
- **2 NCIA or DLSw** packets on **TCP port 2067** for ACE line 30
- **8 PPTP** packets on **TCP port 1723** for ACE line 31
- **3 XOT or X.25 Routing** packets on **TCP port 1998** for ACE line 32
- **4 Cisco CME** packets on **TCP port 3804** for ACE line 33
- **3 SIP Gateway Signaling** packets on **TCP port 2443** for ACE line 34
- **20 SIP** packets on **TCP ports 5060 and 5061** for ACE line 35
- **8 HTTP** packets on **TCP port 80** for ACE line 36
- **3 HTTPS** packets on **TCP port 443** for ACE line 37

- **7 DNS** packets on **TCP port 53** for ACE line 38

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 vulnerabilities that are 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
Mar 25 2009 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.18/2944
dst inside:192.168.60.191/3804 by access-group "tACL-Policy"
Mar 25 2009 00:15:13: %ASA-4-106023: Deny tcp src outside:192.2.0.200/2945
dst inside:192.168.60.33/1983 by access-group "tACL-Policy"
Mar 25 2009 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.99/2946
dst inside:192.168.60.240/1982 by access-group "tACL-Policy"
Mar 25 2009 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.100/2947
dst inside:192.168.60.115/5061 by access-group "tACL-Policy"
Mar 25 2009 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.88/2949
dst inside:192.168.60.38/1981 by access-group "tACL-Policy"
Mar 25 2009 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.175/2950
dst inside:192.168.60.250/2443 by access-group "tACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL *tACL-Policy* show **Cisco CME** packets for **TCP port 3804**, **SIP** packets for **TCP port 5061**, **DLSw** packets for **TCP port 1981, 1982 and 1983** and **SIP Gateway** packets for **TCP port 2443** sent to the address block assigned to the infrastructure 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.

Additional Information

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND

OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

Revision History

Revision 1.0	2009-MARCH-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. 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](#)
- [Understanding Control Plane Protection](#)
- [Securing Tool Command Language on Cisco IOS](#)
- [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)

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.](#)