

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

Applied Mitigation Bulletins

# Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Multiple Vulnerabilities in Cisco IOS While Processing SSL Packets

<http://www.cisco.com/warp/public/707/cisco-amb-20070522-SSL.shtml>

## Revision 1.0

For Public Release 2007 May 22 1300 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 *Multiple Vulnerabilities in Cisco IOS While Processing SSL Packets* and provides identification and mitigation techniques that administrators can deploy on Cisco devices within a network.

### Vulnerability Characteristics

Multiple vulnerabilities exist in IOS when processing malformed SSL packets. These vulnerabilities are summarized as follows:

**Processing ClientHello messages:** This vulnerability can be exploited remotely without authentication and without user interaction. 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 vector used to exploit this vulnerability is through SSL using TCP port 443. At the time of publication, there was no CVE ID associated with this vulnerability.

**Processing ChangeCipherSpec messages:** This vulnerability can be exploited remotely without authentication and without user interaction. 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 vector used to exploit this vulnerability is through SSL using TCP port 443. At the time of publication, there was no CVE ID associated with this vulnerability.

**Processing Finished messages:** This vulnerability can be exploited remotely without authentication and without user interaction. 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 vector used to exploit this vulnerability is through SSL using TCP port 443. At the time of publication, there was no CVE ID associated with this vulnerability.

This document contains information to assist Cisco customers in mitigating attempts to exploit the vulnerabilities in Cisco IOS while processing SSL packets. Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisory:<http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>

## Mitigation Technique Overview

Cisco devices provide several countermeasures for the vulnerabilities described in this document. Many of these protection methods should be considered general security best practices for infrastructure devices and the traffic that transits the network.

Cisco IOS Software can provide effective means of exploit prevention using infrastructure access control lists. Effective means of exploit prevention can also be provided by Cisco ASA 5500 Series Adaptive Security Appliance, 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. These protection mechanisms filter and drop packets attempting to exploit the vulnerabilities described in this document.

The Cisco Intrusion Prevention System provides visibility into and protection against attacks trying to exploit one of the vulnerabilities described in this document through the effective use of event actions.

Visibility into these exploitation attempts can be provided by Cisco IOS NetFlow using flow records as well as by Cisco IOS Software, Cisco ASA, Cisco PIX, and FWSM firewalls through syslog messages and the counter values displayed in the output from **show** commands. Visibility can also be provided using the Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance through the use of queries and event reporting.

## Risk Management

Organizations should follow their standard risk mitigation process to determine the potential impact of these vulnerabilities. Documents that may be used to aid in risk triage are available at [Risk Triage for Security Vulnerability Announcements](#) and [Risk Triage and Prototyping](#).

## 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 on mitigation and identification is available for these devices:

- [Cisco IOS Routers and Switches](#)
- [Cisco IOS NetFlow](#)
- [Cisco ASA, PIX, and FWSM Firewalls](#)
- [Cisco Intrusion Prevention System](#)
- [Cisco Security Monitoring, Analysis, and Response System](#)

## Cisco IOS Routers and Switches

### Mitigation: Infrastructure Access Control Lists

In an effort to protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, infrastructure access control lists (iACLs) should be deployed to perform policy enforcement of traffic sent to infrastructure equipment. The construction of an iACL is accomplished 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.

In the following example, the address block 192.168.1.0/24 is the infrastructure address space and the host at 192.168.100.1 is considered a trusted endpoint. The iACL policy denies SSL packets on TCP port 443 sent to addresses that are part of the infrastructure address space. Care should be taken to allow required traffic for routing and administrative access prior to denying all traffic sent directly to infrastructure devices. Whenever possible, infrastructure address space should be distinct from the address spaced 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 at [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 port(s)
!
permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 443
!
!-- The following vulnerability-specific access control entries
!-- (ACEs) can aid in identification of attacks
!
deny tcp any 192.168.1.0 0.0.0.255 eq 443
!
!-- Explicit default deny ACE for traffic sent to addresses
!-- configured within the infrastructure address space
!
deny ip any 192.168.1.0 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 interface(s) in the ingress direction
!
interface FastEthernet0
 ip access-group infrastructure-acl-policy in
!
```

Please note that filtering traffic with an interface access list will elicit the transmission of ICMP unreachable messages back to the source of the filtered traffic. This could have the undesired side effect of high CPU utilization because the device needs to generate these ICMP unreachable messages. In IOS, ICMP unreachable generation is limited by default to one packet per 500 ms. Administrators can disable ICMP unreachable generation using the **no ip unreachable** interface configuration command. ICMP unreachable rate limiting can be changed using the global configuration command **ip icmp rate-limit unreachable *interval-in-ms***.

### Identification: Infrastructure Access Control Lists

Once the infrastructure ACL has been applied to an interface, administrators can use the **show ip access-lists** command to identify the number of SSL packets on TCP port 443 that have been filtered. Filtered packets should be investigated to determine whether they are attempts to exploit one of 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 192.168.100.1 192.168.1.0 0.0.0.255 eq 443
 20 deny tcp any 192.168.1.0 0.0.0.255 eq 443 (18 matches)
 30 deny ip any 192.168.1.0 0.0.0.255
router#
```

In the preceding example, the access list *infrastructure-acl-policy* has dropped **18 SSL packets** on TCP port 443 for ACE sequence ID 20.

### Identification: Access List Logging

The **log** or **log-input** 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 (ACL) logging can be very CPU intensive and must be used with extreme caution. The CPU impact from ACL logging is driven by two factors: process switching as a result of packets matching **log**-enabled ACEs and log generation and transmission.

The CPU impact from ACL logging can be addressed in hardware on the Catalyst 6500 Series switches and Cisco 7600 Series routers with Supervisor 720 and Supervisor 32 using optimized ACL logging.

The **ip access-list logging interval *interval-in-ms*** command can limit the effects of ACL logging-induced process switching. The **logging rate-limit *rate-per-second* [except *loglevel*]** command limits the impact of log generation and transmission.

## Cisco IOS NetFlow

### Identification: Traffic Flow Identification Using NetFlow Records

Cisco IOS NetFlow can be configured on Cisco IOS routers and switches to aid in the identification of traffic flows that may be potential attempts to exploit the vulnerabilities described in this document. Flows should be investigated to determine whether they are attempts to exploit one of these vulnerabilities or whether the flows are legitimate traffic.

```
switch#show ip cache flow
-----
MSFC:
```

IP packet size distribution (68767 total packets):

```

1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 48
.004 .893 .100 .000 .000 .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, 4456704 bytes  
 88 active, 65448 inactive, 48338 added  
 902532 aged polls, 0 flow alloc failures  
 Active flows timeout in 30 minutes  
 Inactive flows timeout in 15 seconds

IP Sub Flow Cache, 270664 bytes  
 176 active, 16208 inactive, 96675 added, 48338 added to flow  
 0 alloc failures, 0 force free  
 1 chunk, 1 chunk added  
 last clearing of statistics never

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Se /Flow
TCP-Telnet	28	0.0	5	42	0.0	7.6	13.3
TCP-WWW	23	0.0	1	45	0.0	4.3	9.2
TCP-Frag	508	0.0	1	40	0.0	0.0	15.3
TCP-other	40528	0.0	1	47	0.0	2.9	15.4
UDP-NTP	1	0.0	4	96	0.0	0.0	15.5
UDP-other	310	0.0	1	29	0.0	0.0	15.4
ICMP	6852	0.0	1	83	0.0	0.0	15.4
Total:	48250	0.0	1	51	0.0	2.4	15.4

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pk
Vl150	192.168.17.18	Vl200	192.168.41.21	06	2BF6	E5FD	1
Vl150	192.168.150.60	Vl200	192.168.172.1	06	A783	6A4E	2
Vl150	192.168.13.2	Vl200	192.168.1.74	06	ECEF	5709	3
<b>Vl150</b>	<b>192.168.16.7</b>	<b>Vl200</b>	<b>192.168.1.21</b>	<b>06</b>	<b>7584</b>	<b>01BB</b>	<b>1</b>
Vl150	192.168.150.60	Vl200	192.168.1.38	06	38CC	F32A	1
Vl150	192.168.50.150	Vl200	192.168.1.21	06	0A84	8B9F	5
<b>Vl150</b>	<b>192.168.149.38</b>	<b>Vl200</b>	<b>192.168.1.21</b>	<b>06</b>	<b>7B1F</b>	<b>01BB</b>	<b>1</b>
Vl150	192.168.150.60	Vl200	192.168.1.193	06	20B5	FEFF	1
<b>Vl150</b>	<b>192.168.150.60</b>	<b>Vl200</b>	<b>192.168.1.21</b>	<b>06</b>	<b>DE40</b>	<b>01BB</b>	<b>9</b>
<b>Vl150</b>	<b>192.168.15.227</b>	<b>Vl200</b>	<b>192.168.1.21</b>	<b>06</b>	<b>390D</b>	<b>01BB</b>	<b>1</b>
<b>Vl150</b>	<b>192.168.3.17</b>	<b>Vl200</b>	<b>192.168.1.52</b>	<b>06</b>	<b>C976</b>	<b>01BB</b>	<b>6</b>
Vl150	192.168.150.60	Vl200	192.168.1.209	06	CBF3	259A	1

In the preceding example, there are multiple flows for packets on TCP port 443 (Hex value 01BB). This traffic is being sent to addresses within the 192.168.1.0/24 address block, which is used for infrastructure devices. These flows should be compared to baseline utilization for traffic sent to TCP port 443 and they should also be investigated to determine whether the flows are sourced from untrusted host(s) and/or network(s).

To view only the traffic destined for TCP port 443 (Hex value 01BB), the command **show ip cache flow | include SrcIf|\_06\_....\_01BB** may be used to display these NetFlow records, as shown here:

```
switch#show ip cache flow | include SrcIf|_06_...._01BB
```

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pk
Vl32	192.168.32.60	Vl200	192.168.1.112	06	9A8E	01BB	1
Vl150	192.168.150.12	Vl200	192.168.1.29	06	9BE5	01BB	5
Vl10	192.168.10.60	Vl200	192.168.1.15	06	450B	01BB	8
Vl45	192.168.45.13	Vl200	192.168.1.215	06	4671	01BB	1

switch#

## Cisco ASA, PIX, and FWSM Firewalls

## Mitigation: Transit Access Control Lists

In an effort 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 should 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.

The tACL policy denies unauthorized SSL packets on TCP port 443 sent to affected devices. In the following example, 192.168.1.0/24 is the network IP address space used by the affected devices and the host at 192.168.100.1 is considered a trusted source requiring 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 at [Transit Access Control Lists: Filtering at Your Edge](#).

```

!-- Include any explicit permit statements for trusted sources
!-- that require access on the vulnerable port(s)
!
access-list transit-acl-policy extended permit tcp host 192.168.100.1 192.16
!
!-- The following vulnerability-specific ACE can aid
!-- in identification of attacks
!
access-list transit-acl-policy extended deny tcp any 192.168.1.0 255.255.255
!
!-- 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

Once the transit ACL has been applied to an interface, the **show access-list** command can be used to identify the number of SSL packets on TCP port 443 that have been filtered. Filtered packets should be investigated to determine whether they are attempts to exploit one of the vulnerabilities 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
access-list transit-acl-policy line 2 extended deny tcp any 192.168.1.0 255.
access-list transit-acl-policy line 3 extended deny ip any any (hitcnt=8)0x8
Firewall#

```

In the preceding example, the access list *transit-acl-policy* has dropped **205 SSL packets for 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.

## Identification: Firewall Access List Syslog Messages

Firewall syslog message 106023 will be generated for packets denied by an ACE that does not have the **log** keyword present. Additional information about this syslog message is available at [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 at [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 at [Configuring Monitoring and Logging on the Cisco FWSM](#).

In the following examples, the **show logging | grep regex** command is used to extract syslog messages from the logging buffer on the firewall. This is performed to obtain additional information about denied packets that could indicate potential attempts to exploit the vulnerabilities described in this document. It is possible to use different regular expressions with the **grep** keyword to search for specific data within the logged messages.

Additional information on regular expression syntax is available at [Using the Command Line Interface](#).

```
firewall#show logging | grep 106023
Feb 21 2007 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.2.18/2944
Feb 21 2007 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.3.200/2945
Feb 21 2007 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.2.99/2946
Feb 21 2007 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.2.100/2947
Feb 21 2007 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.4.88/2949
Feb 21 2007 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.3.175/2950
firewall#
```

In the preceding example, the messages logged for the tACL *transit-acl-policy* show SSL packets for TCP port 443 sent to the address block assigned to the network infrastructure.

Additional information about syslog messages for ASA and PIX security appliances is available at [Cisco Security Appliance System Log Messages](#). Additional information about syslog messages for the FWSM is available at [Catalyst 500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages](#).

## Cisco Intrusion Prevention System

### Mitigation: IPS Signature Event Actions

The Cisco Intrusion Prevention System (IPS) appliances and services modules can be used to provide threat detection and help prevent attempts to exploit the processing ClientHello messages vulnerability described in this document. Starting with signature update S81 for sensors running Cisco IPS version 6.x or 5.x, the processing ClientHello messages vulnerability described in this document can be detected by signature 5403/0 (signature name: OpenSSL SSL/TLS Malformed Handshake DoS). Signature 5403 is enabled by default, triggers a Medium severity event, has a signature fidelity rating (SFR) of 85, and is configured with a default event action of **produce-alert**. This signature fires when a specific malformed TLS client handshake packet to TCP port 443 (HTTPS) is detected. Firing of this signature may indicate a potential exploit of this vulnerability against an IOS device.

Cisco IPS sensors can be configured to perform an event action upon detection of an attack. The configured event action performs preventive or deterrent controls to help protect against an attack

that is attempting to exploit the processing ClientHello messages vulnerability. The establishment of the three-way TCP handshake is required to exploit this vulnerability, which reduces the possibility of successful attacks using spoofed IP addresses as well as false positive events for signature 5403/0.

Cisco IPS sensors are most effective when deployed in inline protection mode coupled with the use of an event action. Additional information about the risk rating and the calculation of its value is available at [Cisco IPS Risk Rating Explained](#).

Cisco IPS 5.x and 6.x sensors deployed in inline protection mode will need to have an event action configured on a per-signature basis. Alternatively, administrators can configure an override to perform an event action for signatures that trigger and are calculated as a high-risk threat. Using the **deny-packet-inline** or **deny-attacker-inline** event actions on sensors deployed in inline protection mode provides the most effective exploit prevention.

## Cisco Security Monitoring, Analysis, and Response System

### Identification: Cisco Security MARS Query Type and Keyword

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can query on events for the processing ClientHello messages vulnerability using a query type and keyword. Using a keyword of **NR-5403/0** for the Cisco IPS signature 5403/0 (signature name: OpenSSL SSL/TLS Malformed Handshake DoS) and a query type of **All Matching Event Raw Messages** on the Cisco Security MARS appliance will provide a report that list the events created by IPS signature 5403/0.

The following screen shot shows the values used to query for events created by Cisco IPS signature 5403/0.

The screenshot shows the Cisco Security MARS Query interface in a Microsoft Internet Explorer browser window. The address bar shows the URL: <https://10.86.225.42/Query/index.jsp>. The interface includes a navigation menu with tabs for SUMMARY, INCIDENTS, QUERY / REPORTS (selected), RULES, MANAGEMENT, ADMIN, and HELP. Below the navigation menu, there are buttons for Query, Batch Query, and Report. The current user is identified as Administrator (onadmin) with a Logout and Activate button. The interface is titled "Load Report as On-Demand Query with Filter" and shows a "Query Event Data" section with the following configuration:

Query type: Event Raw Messages ranked by Time, 1d-0h [Edit] [Clear]

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-5403/0	None	ANY	ANY

Buttons for "Save As Report", "Save As Rule", and "Submit Inline" are visible at the bottom of the configuration area. The footer of the page contains copyright information: "Copyright © 2003, 2006 Cisco Systems, Inc. All rights reserved." and a navigation menu: "Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help :: Feedback".

The following screen shot shows the query results for **NR-5403/0** created by the Cisco Security MARS appliance using a query type and keyword regex query.

Copyright © 2003, 2006 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help :: Feedback

## 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	2007-May-22	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](#)
- [Protecting Your Core: Infrastructure Protection Access Control Lists](#)
- [Transit Access Control Lists: Filtering at Your Edge](#)
- [Cisco Network Foundation Protection White Papers](#)
- [Cisco IOS NetFlow](#)
- [Cisco Security Appliance System Log Messages, Version 7.2](#)
- [Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages, 3.1](#)
- [Understanding ACL on Catalyst 6500 Series Switches](#)
- [Cisco 6.x Intrusion Prevention System](#)
- [Cisco IPS Risk Rating Explained](#)
- [Cisco IPS 6.x Signature Downloads](#) ( [registered](#) customers only)
- [Cisco IPS 5.x Signature Downloads](#) ( [registered](#) customers only)
- [Cisco Security Monitoring, Analysis, and Response System \(Cisco Security MARS\)](#)

---

### 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.](#)