

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

Applied Mitigation Bulletins

# Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Denial of Service Vulnerabilities in Content Switching Module

<http://www.cisco.com/warp/public/707/cisco-amb-20070905-csm.shtml>

## Revision 1.1

Last Updated 2007 September 12 1600 UTC (GMT)

For Public Release 2007 September 5 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 Advisory *Denial of Service Vulnerabilities in Content Switching Module* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

### Vulnerability Characteristics

There are multiple vulnerabilities in the Cisco Content Switching Module (CSM) and Cisco Content Switching Module with SSL (CSM-S). These vulnerabilities are summarized in the following subsections:

**TCP Packet Processing DoS:** 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 for exploitation is through packets that use TCP. This vulnerability has been assigned CVE name CVE-2007-4788.

**Service Termination:** 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 for exploitation is through packets that use TCP. This vulnerability is susceptible to exploitation through spoofed attacks. This vulnerability has been assigned CVE name CVE-2007-4789.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisory, which is available at the following link: <http://www.cisco.com/warp/public/707/cisco-sa-20070905-csm.shtml>.

## Mitigation Technique Overview

Cisco devices provide several countermeasures for the TCP packet processing DOS and service termination vulnerabilities. Administrators are advised to consider many of these protection methods to be 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 Unicast Reverse Path Forwarding (Unicast RPF). This protection mechanism filters and drops, as well as verifies the source IP address of, packets that are attempting to exploit the service termination vulnerability described in this document. The proper deployment and configuration of Unicast RPF provides the most effective means of protection against attacks that use packets with spoofed source IP addresses. Unicast RPF should be deployed as close to all traffic sources as possible.

Effective means of 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 the following:

- Application Layer Protocol Inspection
- Unicast RPF
- Spoofing protection and embryonic connection limiting using TCP Intercept

These protection mechanisms filter and drop, as well as verify the source IP address of, packets that are attempting to exploit the vulnerabilities described in this document.

The proper deployment and configuration of Unicast RPF provides the most effective means of protection against attacks that use packets with spoofed source IP addresses. Unicast RPF should be deployed as close to all traffic sources as possible.

Effective use of Cisco Intrusion Prevention System (IPS) event actions provides visibility into and protection against attacks that attempt to exploit these vulnerabilities.

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.

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can also provide visibility through queries and event reporting.

## Risk Management

Organizations should 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 in Information Security Engagements](#) can help organizations develop repeatable security evaluation and response processes.

## Device-Specific Mitigation and Identification



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

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

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

### Cisco IOS Routers and Switches

#### Mitigation: Spoofing Protection Using Unicast Reverse Path Forwarding

The service termination vulnerability described in this document can be exploited by spoofed IP packets. Administrators can deploy and configure Unicast Reverse Path Forwarding (Unicast RPF) as a protection mechanism against spoofing. The proper deployment and configuration of Unicast RPF can provide protection mechanisms against spoofing related to the service termination vulnerability.

Unicast RPF is configured at the interface level and can detect and drop packets that lack a verifiable source IP address. Administrators should not rely on Unicast RPF to provide 100 percent spoofing protection because spoofed packets may enter the network through a Unicast RPF-enabled interface if an appropriate return route to the source IP address exists. Administrators should take care to ensure that the appropriate Unicast RPF mode (loose or strict) is configured during the deployment of this feature because it can drop legitimate traffic that is transiting the network. In an enterprise environment, Unicast RPF might be enabled at the Internet edge and the internal access layer on the user-supporting Layer 3 interfaces.

Additional information is available in the [Unicast Reverse Path Forwarding Loose Mode Feature Guide](#).

For additional information about the configuration and use of Unicast RPF, reference the [Understanding Unicast Reverse Path Forwarding](#) Applied Intelligence white paper.

### Identification: Spoofing Protection Using Unicast Reverse Path Forwarding

With Unicast RPF properly deployed and configured throughout the network infrastructure, administrators can use the **show ip interface**, **show cef drop**, **show cef interface type slot/port internal**, and **show ip traffic** commands to identify the number of packets that Unicast RPF has dropped.

NOTE: The **show command | begin regexp** and **show command | include regexp** command modifiers are used in the following examples to minimize the amount of output that administrators need to parse to view the desired information. Additional information about command modifiers is available in the [show command](#) sections of the Cisco IOS Configuration Fundamentals Command Reference.

NOTE: **show cef interface type slot/port internal** is a hidden command that must be fully entered at the command-line interface. Command completion is not available for it.

```
router#show ip interface GigabitEthernet 0/0 | begin verify
--          CLI Output Truncated          --

      IP verify source reachable-via RX, allow default, allow self-ping
      18 verification drops
      0 suppressed verification drops
router#

router#show cef drop
CEF Drop Statistics

Slot  Encap_fail  Unresolved  Unsupported  No_route  No_adj  ChkSum_Err
RP    27           0           0           18        0       0

IPv6 CEF Drop Statistics

Slot  Encap_fail  Unresolved  Unsupported  No_route  No_adj
RP    0           0           0           3         0

router#

router#show cef interface GigabitEthernet 0/0 internal | include drop
--          CLI Output Truncated          --

      ip verify: via=rx (allow default), acl=0, drop=18, sdrop=0, allow self-ping
router#

router#show ip traffic

IP statistics:

Rcvd:  68051015 total, 2397325 local destination
       43999 format errors, 0 checksum errors, 33 bad hop count
       2 unknown protocol, 929 not a gateway
       21 security failures, 190123 bad options, 542768 with options
Opts:  352227 end, 452 nop, 36 basic security, 1 loose source route
```

```

45 timestamp, 59 extended security, 41 record route
53 stream ID, 3 strict source route, 40 alert, 45 cipso, 0 ump
361634 other
Frag: 0 reassembled, 10008 timeouts, 56866 couldn't reassemble
0 fragmented, 0 fragments, 0 couldn't fragment
Bcast: 64666 received, 0 sent
Mcast: 1589885 received, 2405454 sent
Sent: 3001564 generated, 65359134 forwarded
Drop: 4256 encapsulation failed, 0 unresolved, 0 no adjacency
      18 no route, 18 unicast RPF, 0 forced drop
      0 options denied
Drop: 0 packets with source IP address zero
Drop: 0 packets with internal loop back IP address

--      CLI Output Truncated      --

router#
```

In the preceding examples, Unicast RPF has dropped **18 IP packets** received globally on all interfaces with Unicast RPF configured because of the inability to verify the source address of the IP packets within the Cisco Express Forwarding Forwarding Information Base.

## Cisco ASA, PIX, and FWSM Firewalls

### Mitigation: Application Layer Inspection

The ASA and PIX [HTTP application inspection](#) feature will prevent exploitation of the TCP packet processing DoS vulnerability. The CSM and CSM-S modules define [virtual servers \(vserver\)](#) as the entities that are subject to load balancing. The virtual servers are the entities that can be exploited by the vulnerabilities described in this document.

In the following example, 192.168.1.170, 192.168.130.68, and 192.168.150.70 are the IP addresses of the virtual servers configured in the affected CSM or CSM-S. The first two virtual servers provide HTTP and HTTPS services. The last virtual server permits access to an FTP server farm.

```

!
!
!--- Create an access list that will be used to identify traffic
!--- to the CSM virtual servers that will be protected.
!
access-list CSM-VServer-Web extended permit tcp any host 192.168.1.170 eq www
access-list CSM-VServer-Web extended permit tcp any host 192.168.130.68 eq http
!
access-list CSM-VServer-FTP extended permit tcp any host 192.168.150.70 eq ftp
!
!
!--- Create a class map for each type of traffic that will be inspected.
!
class-map CSM-Web
  match access-list CSM-VServer-Web
class-map CSM-FTP
  match access-list CSM-VServer-FTP
!
```

```

!--- Apply appropriate inspection to the traffic classes.

!
policy-map global_policy
  class CSM-Web
    inspect http
  class CSM-FTP
    inspect ftp

service-policy global_policy global

```

### **Mitigation: Spoofing Protection Using Unicast Reverse Path Forwarding**

The service termination vulnerability described in this document may be exploited by spoofed IP packets. Administrators can deploy and configure Unicast RPF as a protection mechanism against spoofing.

Unicast RPF is configured at the interface level and can detect and drop packets that lack a verifiable source IP address. Administrators should not rely on Unicast RPF to provide 100 percent spoofing protection because spoofed packets may enter the network through a Unicast RPF-enabled interface if an appropriate return route to the source IP address exists. In an enterprise environment, Unicast RPF might be enabled at the Internet edge and at the internal access layer on the user-supporting Layer 3 interfaces.

For additional information about the configuration and use of Unicast RPF, reference the Cisco Security Appliance Command Reference for [ip verify reverse-path](#) and the [Understanding Unicast Reverse Path Forwarding](#) Applied Intelligence white paper.

### **Mitigation: Spoofing Protection and Embryonic Connection Limiting with TCP Intercept**

The service termination vulnerability can be exploited through packets with spoofed source IP addresses. The CSM Service Termination feature is designed to protect against DoS attacks. Similar functionality can be obtained using the ASA TCP Intercept feature. Both features use SYN cookies to minimize the memory and CPU load to protect against a high rate of spoofed connection attempts.

When SYN cookies are used, the firewall or load-balancing device responds to incoming connection requests (SYNs) with a specially crafted TCP SYN ACK packet. This TCP SYN ACK packet has a cookie integrated into the TCP header sequence number field. The cookie encodes the minimal aspects of the initial connection request and the firewall or load-balancing device does not keep any state of the initial TCP SYN packet. This function is particularly important because it prevents state from being created on the firewall when it is under a spoofing attack.

If the crafted SYN ACK reaches a valid remote device, the remote device will ACK the SYN ACK as the final step of the three-way handshake used by TCP. When the firewall or load-balancing device receives the TCP ACK packet, it looks for the cookie in the TCP header sequence number. If the cookie is valid, the firewall has validated the connection and will then proceed to create the TCP back-end connection to the destination host using the TCP MSS value obtained from the cookie.

Note that SYN cookies are used in the ASA, PIX, and FWSM when there is at least one other connection already established in the network address translation (NAT) mapping or associated class map.

There are two considerations when using SYN cookies:

- The SYN cookie encodes a set of predefined TCP MSS values.
- The SYN cookie prevents the use of any TCP option other than TCP MSS.

The ASA TCP Intercept feature provides a more granular level of protection against spoofed IP packets than that of Unicast RPF. This form of protection can be configured through the use of static NAT or static identity NAT for ASA, PIX, and FWSM firewalls. In addition, the ASA firewall may be configured through the use of the Modular Policy Framework (MPF). These three forms of spoofing protection and embryonic connection limiting using the TCP Intercept feature are detailed in this section:

- Static NAT
- Static identity NAT
- Modular Policy Framework

### Static NAT

Static NAT creates a static IP-to-IP NAT mapping. Static NAT configuration capabilities allow administrators to set embryonic connection limits and also to limit the maximum number of connections. In the following example, an embryonic connection limit of *1* will be set. This limit will force all but the first concurrent TCP connection to be validated using SYN cookies. Note that setting the embryonic limit to zero disables the TCP Intercept feature.

The following command will statically map the inside IP address 192.168.1.170 to the outside IP address 192.0.2.10 and will create an embryonic connection limit of *1*. The [static](#) command is available on ASA, PIX, and FWSM firewalls.

```
static (inside,outside) 192.0.2.10 192.168.1.170 tcp 0 1
```

### Static Identity NAT

Static identity NAT creates a static IP-to-IP mapping without performing IP address translation. The benefit of using static identity NAT is the ability to set embryonic connection limits and also to limit the maximum number of connections as if static IP address translations were taking place. In the following example, an embryonic connection limit of *1* will be set, which will in effect force all TCP connections to be validated using SYN cookies after the embryonic connection threshold is reached.

The following command will statically map the entire 192.168.150.0/24 subnet to itself and will create an embryonic connection limit of *1*. The [static](#) command is available on ASA, PIX, and FWSM firewalls.

```
static (inside,outside) 192.168.150.0 192.168.150.0 netmask 255.255.255.0 tcp 0
```

### Modular Policy Framework

Administrators can also implement TCP Intercept using the Modular Policy Framework (MPF). Although MPF is available on the FWSM, the configuration of TCP Intercept using MPF and the **set connection** command is possible only on the ASA and PIX firewalls.

TCP Intercept using MPF is available on the ASA firewall using the [set connection](#) command. In the following example, an embryonic connection limit of 1 will be set. The following commands will create an embryonic connection limit of 1 for the web servers with the IP addresses 192.168.1.170 and 192.168.130.68 and for the FTP server at the IP address 192.168.150.70.

```

!
!--- Create an access list that will be used to identify traffic
!--- to the CSM virtual servers that will be protected.

!
access-list CSM-VServer-Web extended permit tcp any host 192.168.1.170 eq www
access-list CSM-VServer-Web extended permit tcp any host 192.168.130.68 eq http
access-list CSM-VServer-FTP extended permit tcp any host 192.168.150.70 eq ftp
!

!--- Create a class map for each type of traffic that will be inspected.

!
class-map CSM-Web
 match access-list CSM-VServer-Web
class-map CSM-FTP
 match access-list CSM-VServer-FTP
!

!--- Apply appropriate inspection to the traffic classes.

!
policy-map global_policy
 class CSM-Web
  set connection embryonic-conn-max 1
 class CSM-FTP
  set connection embryonic-conn-max 1
!
service-policy global_policy global

```

Note that both inspection and setting of a maximum embryonic connection can be used in the same service policy to minimize the risk of exploitation of the TCP packet processing DoS and service termination vulnerabilities. The complete configuration follows:

```

!
!--- Create an access list that will be used to identify traffic
!--- to the CSM virtual servers that will be protected.

!
access-list CSM-VServer-Web extended permit tcp any host 192.168.1.170 eq www
access-list CSM-VServer-Web extended permit tcp any host 192.168.130.68 eq http
!

access-list CSM-VServer-FTP extended permit tcp any host 192.168.150.70 eq ftp
!

!--- Create a class map for each type of traffic that will be inspected.

!
class-map CSM-Web
 match access-list CSM-VServer-Web

```

```

class-map CSM-FTP
  match access-list CSM-VServer-FTP

!

!--- Apply appropriate inspection to the traffic classes.

!
policy-map global_policy
  class CSM-Web
    inspect http
    set connection embryonic-conn-max 1
  class CSM-FTP
    inspect ftp
    set connection embryonic-conn-max 1
!
service-policy global_policy global

```

### Identification: Spoofing Protection Using Unicast Reverse Path Forwarding

Firewall syslog message *106021* will be generated for packets denied by Unicast RPF. Additional information about this syslog message is available in [Cisco Security Appliance System Log Message - 106021](#).

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 attempts to exploit the service termination 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 106021
Feb 21 2007 00:15:13: %ASA-1-106021: Deny UDP reverse path check from 192.168.0
Feb 21 2007 00:15:13: %ASA-1-106021: Deny UDP reverse path check from 192.168.0
Feb 21 2007 00:15:13: %ASA-1-106021: Deny TCP reverse path check from 192.168.0
firewall#

```

The **show asp drop** command can also identify the number of packets that Unicast RPF has dropped, as shown in the following example:

```

firewall#show asp drop

Frame drop:
  Reverse-path verify failed                11
  Flow is denied by configured rule        855
  Expired flow                             1
  Interface is down                        2

```

```
Flow drop:
```

```
firewall#
```

In the preceding example, Unicast RPF has dropped **11 IP packets** received on interfaces with Unicast RPF configured. For additional information about the configuration and use of Unicast RPF, reference the Cisco Security Appliance Command Reference for [show asp drop](#).

## Cisco Intrusion Prevention System

### Mitigation: Cisco IPS Signature Event Actions

Administrators can use the Cisco Intrusion Prevention System (IPS) appliances and services modules to provide threat detection and help prevent attempts to exploit the vulnerabilities described in this document. These vulnerabilities may be detected by the following signatures:

- Signature 1300/0 - TCP Segment Overwrite (S212)
- Signature 6009/0 - SYN Flood DOS (S214)

#### Signature 1300/0 - TCP Segment Overwrite (S212)

Starting with signature update S212 for sensors running Cisco IPS version 6.x or 5.x, the TCP packet processing DoS vulnerability described in this document can be detected by signature 1300/0 (Signature Name: TCP Segment Overwrite). Signature 1300/0 is enabled by default, triggers a *High* severity event, has a signature fidelity rating (SFR) of 100, and is configured with default event actions of **Deny Connection Inline** and **Produce Alert**. Signature 1300/0 fires when one or more TCP segments in the same stream overwrite data from one or more segments located earlier in the stream. Firing of this signature may indicate a potential exploit of the TCP packet processing DoS vulnerability described in this document.

#### Signature 6009/0 - SYN Flood DOS (S214)

Starting with signature update S214 for sensors running Cisco IPS version 6.x or 5.x, the service termination vulnerability described in this document can be detected by signature 6009/0 (Signature Name: SYN Flood DOS). Signature 6009/0 is not enabled by default, triggers a *Medium* severity event, has an SFR of 85, and is configured with a default event action of **Produce Alert**. Signature 6009/0 fires when a flood of TCP SYN packets at a rate of 100 per second or greater is detected. Firing of this signature may indicate a potential exploit of the service termination vulnerability described in this document.

Administrators can configure Cisco IPS sensors to perform an event action when an attack is detected. The configured event action performs preventive or deterrent controls to help protect against an attack that is attempting to exploit the vulnerabilities described in this document.

Cisco IPS sensors are most effective when deployed in inline protection mode combined with the use of an event action. Automatic Threat Prevention for Cisco IPS 6.x sensors deployed in inline protection mode provides threat prevention against an attack that is attempting to exploit these vulnerabilities. Threat prevention is achieved through a default override that performs an event action of **Deny Connection Inline** and **Produce Alert** for triggered signatures with a riskRatingValue greater than 90. Additional information about the risk rating and the calculation of its value is available in [Cisco IPS](#)

[Risk Rating Explained.](#)**Identification: IPS Signature Events****Signature 1300/0 - TCP Segment Overwrite**

```

sensor6# show event alarm
evIdsAlert: eventId=1184072489279353349 severity=high vendor=Cisco
originator:
  hostId: sensor6x
  appName: sensorApp
  appInstanceId: 395
time: 2007/08/28 11:12:58 2007/08/28 06:12:58 CDT
signature: description=TCP Segment Overwrite id=1300 version=S212
  subsigId: 0
  sigDetails: TCP segment overwrites payload data in previous 256 bytes
  marsCategory: Penetrate/Evasion/TCPIP
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=OUT 192.168.208.170
    port: 27328
  target:
    addr: locality=OUT 192.168.1.170
    port: 80
    os: idSource=learned relevance=relevant type=linux
actions:
  denyPacketRequestedNotPerformed: true
  denyFlowRequestedNotPerformed: true
riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 100
threatRatingValue: 100
interface: ge0_0
protocol: tcp

```

**Signature 6009/0 - SYN Flood DOS**

```

evIdsAlert: eventId=1184072489279352876 severity=medium vendor=Cisco
originator:
  hostId: sensor6x
  appName: sensorApp
  appInstanceId: 395
time: 2007/08/28 10:33:26 2007/08/28 05:33:26 CDT
signature: description=SYN Flood DOS id=6009 version=S214
  subsigId: 0
  sigDetails: SYN Flood DOS

  marsCategory: DoS/Host
  marsCategory: DoS/Network/TCP
interfaceGroup: vs3
vlan: 0
participants:
  attacker:
    addr: locality=OUT 192.168.208.219
    port: 44717
  target:
    addr: locality=OUT 192.168.150.70
    port: 21

```

```

os: idSource=learned relevance=relevant type=windows-nt-2k-xp
triggerPacket:
000000 00 18 73 17 9F E8 00 18 74 B5 A4 1A 08 00 45 C0 ..s.....t.....E.
000010 00 2C 00 00 00 00 FE 06 D3 98 C0 A8 D0 DB C0 A8 .,.....
000020 96 46 AE AD 00 15 00 1E 34 2B 00 00 00 00 60 02 .F.....4+.....`.
000030 10 20 C0 23 00 00 02 04 02 18 00 00 ..#.....
riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 73
threatRatingValue: 73
interface: ge0_3
protocol: tcp

```

## Cisco Security Monitoring, Analysis, and Response System

### Identification: Cisco Security Monitoring, Analysis, and Response System Query Type and Keyword

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can query on events for the denial of service vulnerabilities in the Cisco CSM and CSM-S modules using a query type and keywords. Using a keyword of **NR-1300/0** for IPS signature **1300/0**, which may detect the TCP packet processing DoS vulnerability; a keyword of **NR-6009/0** for IPS signature **6009/0**, which may detect the service termination vulnerability; and a query type of **All Matching Event Raw Messages** on the Cisco Security MARS appliance will provide a report that lists the events created by IPS Signatures 1300/0 or 6009/0.

#### 1300/0 - TCP Segment Overwrite

Cisco Security MARS will create an incident if signature TCP Segment Overwrite is triggered. This event could indicate attempts by an attacker to exploit the TCP packet processing DoS vulnerability. Signature 1300/0 triggers events for the Cisco Security MARS event type **TCP Segment Overwrite**.

The following screen shot shows the incident created by Cisco Security MARS.

The screenshot displays the Cisco Security MARS web interface. At the top, there are navigation tabs: SUMMARY, INCIDENTS (selected), QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, and HELP. Below the navigation, the current date and time are shown as 'Aug 28, 2007 7:05:49 PM CDT'. The main header includes 'INCIDENTS | CS-MARS Standalone: R4-MARS v4.2' and a login status for 'Administrator (gnadmin)'. There are buttons for 'View Cases' and 'New Case'. Below this, there are input fields for 'Incident ID: 48576610' and 'Session ID:'. The main content area shows details for a rule named 'System Rule: Misc. Attacks: Evasion' with a status of 'Active' and a time range of '0h:30m'. The description states: 'This correlation rule detects generic attempts by an attacker to bypass network IDS systems. The attempts may be preceded by reconnaissance attempts to that host.' Below the description is a table with columns: Offset, Open, Source IP, Destination IP, Service Name, Event, Device, Reported User, Keyword, Severity, Count, Close, and Operation. The table contains three rows of rule conditions. Below the rule details, there are buttons for 'Expand All' and 'Collapse All'. The incident ID '48576610' is displayed with icons. Below this is a detailed event table with columns: Offset, Session / Incident ID, Event Type, Source IP/Port, Destination IP/Port, Protocol, Time, Reporting Device, Reported User, Path / Mitigate, and Tune. The event table shows a 'TCP Segment Overwrite' event from source IP 192.168.208.170:53378 to destination IP 192.168.150.70:21 on TCP protocol, reported on Aug 28, 2007 5:12:18 AM CDT from device R4-IPS4240a. The event is categorized as 'False Positive Tuning'. At the bottom, there is a copyright notice for Cisco Systems, Inc. and a navigation bar with 'Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help :: Feedback'. A red-bordered box highlights a portion of the event table data.

Offset	Open	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	Close	Operation
1	(	ANY	SAME, \$TARGET01, ANY	ANY	Probe/HostInfo/All, Penetrata/ViewFiles/Sensitive	ANY	None	ANY	ANY	1	)	FOLLOWED-BY
2		ANY	SAME, \$TARGET01, ANY	ANY	Penetrata/Evasion/TCP/IP	ANY	None	ANY	ANY	1	)	OR
3		ANY	SAME, \$TARGET01, ANY	ANY	Penetrata/Evasion/TCP/IP	ANY	None	ANY	ANY	1		

  

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	Tune
3	S:54755586, I:48576610	TCP Segment Overwrite	192.168.208.170 53378	192.168.150.70 21	TCP	Aug 28, 2007 5:12:18 AM CDT	R4-IPS4240a			False Positive Tuning

  

Event Type	Source IP/Port	Destination IP/Port	Protocol
TCP Segment Overwrite	192.168.208.170 53378	192.168.150.70 21	TCP

### 6009/0 - SYN Flood DOS

Cisco Security MARS will create an incident if signature SYN Flood DOS is triggered. This occurs when 100 or more TCP SYN packets per second are detected between the same source IP address and victim destination TCP port. Signature 6009/0 triggers events for the Cisco Security MARS event type

### Half-open SYN Attack / SYN Flood Denial of Service.

The following screen shot shows the incident created by Cisco Security MARS.

The screenshot displays the Cisco Security MARS interface. At the top, there are navigation tabs: SUMMARY, INCIDENTS (selected), QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, and HELP. Below this, there are sub-tabs: Incidents, False Positives, and Cases. The date and time are shown as Aug 28, 2007 6:35:42 PM CDT. The user is logged in as Administrator (pnadmin) with options for Logout and Activate. There are buttons for View Cases and New Case. Incident ID: 48577052 and Session ID: are displayed. Below this is a rule summary for 'System Rule: Server Attack: Misc. - Attempt' with status 'Active' and time range '0h:30m'. The description states: 'This correlation rule detects attacks on miscellaneous services (i.e. other than DNS, FTP, HTTP, Mail, FTP, RPC, Telnet, SSH, R-protocols) on a host, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, remote command execution attempts, privilege escalation attempts to become root, denial of service attempts etc.' A table of events follows, with columns: Offset, Open, Source IP, Destination IP, Service Name, Event, Device, Reported User, Keyword, Severity, Count, Close, and Operation. The table shows three entries. Below the table are buttons for Expand All and Collapse All. At the bottom, there is a table with columns: Offset, Session / Incident ID, Event Type, Source IP/Port, Destination IP/Port, Protocol, Time, Reporting Device, Reported User, Path / Mitigate, and Tune. The first row of this table is highlighted with a red border and contains the following data: Offset 3, Session / Incident ID, Event Type 'Half-open SYN Attack / SYN Flood Denial of Service', Source IP/Port '192.168.150.70', Destination IP/Port '21', Protocol '192.168.208.218', Time '27220', Reporting Device, Reported User, Path / Mitigate, and Tune 'False Positive Tuning'.

The following screen shot shows the values used to query for events created by IPS signature 1300/0

(Signature Name: TCP Segment Overwrite) or signature 6009/0 (Signature Name: SYN Flood DOS).

The screenshot shows the Cisco MARS web interface. At the top, there is a navigation menu with tabs for SUMMARY, INCIDENTS, QUERY / REPORTS (selected), RULES, MANAGEMENT, ADMIN, and HELP. Below this is a sub-menu with Query, Batch Query, and Report. The current date and time are Aug 30, 2007 7:03:57 PM CDT. The user is logged in as Administrator (pnadmin) and can click Logout or Activate. There are buttons for View Cases and New Case.

The main section is titled "Load Report as On-Demand Query with Filter". It has a dropdown menu set to "All" and a "Select Report..." dropdown. To the right, there are input fields for Incident ID and Session ID, each with a "Show" button.

Below this is the "Query Event Data" section, which says "Click the cells below to change query criteria:". The query type is "Event Raw Messages ranked by Time, Aug 25, 2007 6:46:00 PM CDT - Aug 30, 2007 6:56:00 PM CDT". There are "Edit" and "Clear" buttons.

Source IP	Destination IP	Service	Events	Device	Report User	Keyword	ation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-1300/0 OR NR-6009/0		ANY	ANY

Below the table, there are several empty input fields, a dropdown menu set to "ANY", and an "Apply" button. At the bottom of the query section, there are buttons for "Save As Report", "Save As Rule", and "Submit Batch".

At the very bottom of the page, there is a copyright notice: "Copyright © 2003, 2006 Cisco Systems, Inc. All rights reserved." and a breadcrumb trail: "Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help :: Feedback".

The following screen shot shows the query results for **NR-1300/0** or **NR-6009/0** created by the Cisco Security MARS appliance using a query type and keyword regex query.

**CISCO SYSTEMS**

SUMMARY INCIDENTS **QUERY / REPORTS** RULES MANAGEMENT ADMIN HELP

Query Batch Query Report Aug 30, 2007 9:22:11 PM CDT

QUERY / REPORTS | CS-MARS Standalone: R4-MARS v4.2 Login: Administrator (pnadmin) :: Logout :: Activate

View Cases New Case

Report Results (Total): local:pnadmin: Event Types, Aug 30, 2007 9:13:29 PM CDT Aug 30, 2007 7:03:30 PM CDT - Aug 30, 2007 9:13:30 PM CDT

Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
local:pnadmin: Event Types, Aug 30, 2007 9:13:29 PM CDT	Run on demand only	Total View	Administrator (pnadmin)	Keyword: NR-1300/0 OR NR-6009/0 Query Type: Event Types ranked by Sessions Time: 0d-2h:10m	local:pnadmin: Event Types, Aug 30, 2007 9:13:29 PM CDT	In Progress...	Aug 30, 2007 9:13:30 PM CDT	Aug 30, 2007 7:03:00 PM CDT - Aug 30, 2007 9:12:00 PM CDT

Report type: Event Types ranked by Sessions, 0d-2h:10m

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-1300/0 OR NR-6009/0	None	ANY	ANY

Other Views: Total View Current Time Display Report

Rank	Total Sessions	Average / Minute	Description	Device Event ID	Groups
1	32	0.25	Half-open SYN Attack / SYN Flood Denial of Service	CheckPoint Opsec NG FP3: SYN Attack, Cisco IDS 3.1: NR-3050/0: Cisco MySDN IPS Signatures, Cisco IDS 3.1: NR-3050/21: Cisco MySDN IPS Signatures, Cisco IDS 3.1: NR-3050/22: Cisco MySDN IPS Signatures, Cisco IDS 3.1: NR-3050/23: Cisco MySDN IPS Signatures, (42 More...)	DoS/All, DoS/Host, DoS/Network/TCP
2	6	0.05	TCP Segment Overwrite	Cisco IDS 3.1: NR-1300/0: Cisco MySDN IPS Signatures, Cisco IDS 4.0: NR-1300/0: Cisco MySDN IPS Signatures, Cisco IOS 12.2: NR-1300/0: Cisco MySDN IPS Signatures, Cisco IPS 5.x: NR-1300/0: Cisco MySDN IPS Signatures, IntruVert IntruShield 1.5: INTRU-TCP Fragment Overlap with Data Mismatch, (4 More...)	Penetrate/All, Penetrate/Evasion/TCP/IP

1 to 2 of 2 25 per page

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 1.1	2007 Sept 12	Added CVE names to Vulnerability Characteristics section.
Revision 1.0	2007 Sept 5	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

- [Static NAT](#)
- [Static Identity NAT](#)
- [Modular Policy Framework to Validate TCP Connection Attempts](#)
- [Catalyst 6500 CSM Protecting Against Denial-of-Service Attacks](#)
- [Defenses Against TCP SYN Flooding Attacks](#)
- [Applied Mitigation Bulletins](#)
- [Unicast Reverse Path Forwarding](#)
- [Cisco Network Foundation Protection White Papers](#)
- [Cisco Firewall Products - Home Page on Cisco.com](#)
- [Unicast Reverse Path Forwarding Loose Mode](#)
- [Reverse Path Forwarding Enhancements for the Internet Service Provider](#)
- [Cisco 6.x Intrusion Prevention System](#)
- [Cisco IPS Signatures by Release Version](#) ( [registered](#) customers only)
- [Cisco IPS 6.x Signature Downloads](#) ( [registered](#) customers only)
- [Cisco IPS Risk Rating Explained](#)
- [IPS Signatures by Signature ID](#) ( [registered](#) customers only)

---

**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](#).