

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the DoS Vulnerability in Cisco WAAS Software

<http://www.cisco.com/warp/public/707/cisco-amb-20070718-waas.shtml>

Revision 1.1

Last Updated 2007 July 21 1600 UTC (GMT)

For Public Release 2007 July 18 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 Vulnerability in Cisco Wide Area Application Services \(WAAS\) Software](#) and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

There is a vulnerability in Wide Area Application Services (WAAS) software when it processes a flood of TCP SYN packets on port 139 or 445. This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may cause these devices to stop processing all types of traffic, i.e. traffic through the device (data traffic) or traffic terminating on the device (management traffic). This condition may occur when a device running

WAAS software is configured for Edge Services, which use Common Internet File System (CIFS) optimization. Exploitation of this vulnerability could result in a sustained denial of service (DoS) condition. Recovery of the system from this unresponsive state can be accomplished only by resetting or power cycling the affected device. The attack vector for exploitation is a flood of TCP SYN packets using port 139 or 445.

This vulnerability is susceptible to exploitation through spoofed attacks. At the time of publication, there was no CVE ID associated with this vulnerability.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisory: <http://www.cisco.com/warp/public/707/cisco-sa-20070718-waas.shtml>

Mitigation Technique Overview

Cisco IOS Software can provide effective means of exploit prevention using the following methods:

- Transit Access Control Lists
- Unicast Reverse Path Forwarding (Unicast RPF)
- IP Source Guard

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

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 the following:

- Transit Access Control Lists
- Unicast RPF

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

The proper deployment and configuration of Unicast RPF provides the most effective means of protection against attacks with spoofed source IP addresses. Deployment as close to all traffic sources as possible provides maximum effectiveness.

The proper deployment and configuration of IP Source Guard provides the most effective means of protection against attacks with spoofed source MAC addresses.

Because there is the potential that a trusted CIFS networking client could become affected by a worm that does not use packets with spoofed source addresses, Unicast RPF and IP Source Guard do not provide complete protection against this vulnerability.

Although the techniques provided in this document cannot completely mitigate this vulnerability, deploying anti-spoofing technologies such as Unicast RPF and IP Source Guard in conjunction with transit ACLs provides the greatest mitigation possible.

Effective use of Cisco Intrusion Prevention System event actions provides visibility into and protection against attacks that attempt to exploit this vulnerability.

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

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 process 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 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: 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. To mitigate this vulnerability, tACLs should be deployed on devices that reside between CIFS networking clients and affected Wide Area Application Engine (WAE) devices configured for Edge Services, which use CIFS optimization. Because there is some potential that a trusted CIFS networking client could become affected by a worm, a tACL workaround cannot provide complete protection against this vulnerability.

The tACL policy denies unauthorized TCP packets on ports 139 and 445. In the following example, 192.168.1.0/24 is the network IP address space used by CIFS servers. The host at 192.168.100.1 is considered a trusted CIFS networking client that requires access to the CIFS servers through an affected WAE device that is configured for Edge Services, which use CIFS optimization. Note that neither the tACL source nor destination IP addresses are that of the affected Edge WAE device. The tACL is constructed to allow TCP port 139 and 445 traffic only between trusted CIFS servers and trusted CIFS networking clients, which should provide mitigation from worm-affected devices that actively scan random IP addresses. Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic.

Additional information about tACLs is available in [Transit Access Control Lists: Filtering at Your Edge](#).

```
!-- Include any explicit permit statements for trusted sources
!-- requiring access on the vulnerable ports to CIFS servers
!
access-list 150 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 139
access-list 150 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 445
!
!-- The following vulnerability-specific access control entries
!-- (ACEs) can aid in identification of attacks
!
access-list 150 deny tcp any 192.168.1.0 0.0.0.255 eq 139
access-list 150 deny tcp any 192.168.1.0 0.0.0.255 eq 445
!
!-- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations
!
!-- Explicit deny for all other IP traffic
!
access-list 150 deny ip any any
!
!-- Apply tACL to interface(s) in the ingress direction
interface GigabitEthernet0/0
 ip access-group 150 in
!
```

Note that filtering with an interface access list will elicit the transmission of ICMP unreachable messages back to the source of the filtered traffic. This could have the undesired effect of increasing CPU utilization because the device needs to generate these ICMP unreachable messages. 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 icmp unreachables**. ICMP unreachable rate limiting can be changed from the default using the global configuration command **ip icmp rate-limit unreachable *interval-in-ms***.

Mitigation: Anti-Spoof Protections

Unicast RPF

The denial of service vulnerability in Cisco WAAS software can be exploited by spoofed IP packets. Protection mechanisms for anti-spoofing exist through the proper deployment and configuration of Unicast RPF. Unicast RPF is configured at the interface level and can detect and drop packets that lack a verifiable IP source address. Administrators should not rely on Unicast RPF to provide 100 percent anti-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 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 background 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 Applied Intelligence white paper at <http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html>.

IP Source Guard

IP source guard (IPSG) is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering packets based on the DHCP snooping binding database and manually configured IP source bindings. Administrators can use IPSG to prevent attacks from an attacker who attempts to spoof packets by forging the source IP address and/or the MAC address. When properly deployed and configured, IPSG coupled with strict mode Unicast RPF provides the most effective means of anti-spoofing protection.

Additional information about the deployment and configuration of IPSG is available in [Configuring DHCP Features and IP Source Guard](#).

Identification: Transit Access Control Lists

After the administrator applies the tACL to an interface, the **show ip access-lists** command will identify the number of packets destined to TCP ports 139 and 445 that have been filtered. Administrators should investigate filtered packets to determine whether they are attempts to exploit this vulnerability. Example output for **show ip access-lists 150** follows:

```
router#show ip access-lists 150
Extended IP access list 150
 10 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 139 (30 matches)
 20 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 445 (50 matches)
 30 deny tcp any 192.168.1.0 0.0.0.255 eq 139 (10 matches)
 40 deny tcp any 192.168.1.0 0.0.0.255 eq 445 (149 matches)
 50 deny ip any any
router#
```

In the preceding example, access list 150 has dropped **10 TCP packets on port 139** for ACE sequence ID 30 and **149 TCP packets on port 445** for ACE sequence ID 40.

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 logging can be very CPU intensive and must be used with extreme caution. The CPU impact of ACL logging is driven by two factors: process switching as a result of

packets that match 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 process switching induced by ACL logging. The **logging rate-limit** *rate-per-second* [**except** *loglevel*] command limits the impact of log generation and transmission.

For additional information about the configuration and use of ACL logging, reference the Applied Intelligence white paper at <http://www.cisco.com/web/about/security/intelligence/acl-logging.html>.

Identification: Anti-Spoof 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** *regex* and **show command** | **include** *regex* command modifiers are used in the following examples to minimize the amount of output that administrators will 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.

```
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 a total of **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 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 potential attempts to exploit the vulnerability described in this document. Administrators should investigate flows to determine whether they are attempts to exploit this vulnerability or whether they are legitimate traffic flows.

```

router#show ip cache flow
IP packet size distribution (790 total packets):
  1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
    .063 .650 .268 .017 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
      512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
        .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  4 active, 4092 inactive, 491 added
  8636 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25800 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never

```

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
TCP-Telnet	30	0.0	3	40	0.0	8.8	15.4
TCP-WWW	15	0.0	3	40	0.0	8.8	15.4
TCP-other	320	0.0	1	58	0.0	0.5	15.4
ICMP	122	0.0	2	80	0.0	2.0	15.5
TCP-Telnet	11393421	2.8	1	48	3.1	0.0	1.4

TCP-FTP	236	0.0	12	66	0.0	1.8	4.8
TCP-FTPD	21	0.0	13726	1294	0.0	18.4	4.1
TCP-WWW	22282	0.0	21	1020	0.1	4.1	7.3
TCP-X	719	0.0	1	40	0.0	0.0	1.3
TCP-BGP	1	0.0	1	40	0.0	0.0	15.0
TCP-Frag	70399	0.0	1	688	0.0	0.0	22.7
TCP-other	47861004	11.8	1	211	18.9	0.0	1.3
UDP-DNS	582	0.0	4	73	0.0	3.4	15.4
UDP-NTP	287252	0.0	1	76	0.0	0.0	15.5
UDP-other	310347	0.0	2	230	0.1	0.6	15.9
ICMP	11674	0.0	3	61	0.0	19.8	15.5
IPv6INIP	15	0.0	1	1132	0.0	0.0	15.4
GRE	4	0.0	1	48	0.0	0.0	15.3
Total:	59957957	14.8	1	196	22.5	0.0	1.5

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/1	192.0.2.2	Gi0/0	192.168.1.71	06	054A	008B	1
Gi0/1	192.0.2.2	Gi0/0	192.168.1.72	06	0506	008B	1
Gi0/1	192.0.2.2	Gi0/0	192.168.1.73	06	096C	01BD	1
Gi0/1	192.0.2.2	Gi0/0	192.168.1.74	06	058A	01BD	1
Gi0/0	192.168.10.201	Gi0/1	192.168.1.102	11	0984	00A1	1
Gi0/0	192.168.11.54	Gi0/1	192.168.1.158	11	0911	00A1	101
Gi0/1	192.168.150.60	Gi0/0	10.89.16.226	06	0016	12CA	1208
Gi0/0	192.168.13.97	Gi0/1	192.168.1.28	11	0B3E	00A1	55
Gi0/0	192.168.10.17	Gi0/1	192.168.1.97	11	0B89	00A1	112
Gi0/0	10.88.226.1	Gi0/1	192.168.202.22	11	007B	007B	219
Gi0/0	192.168.12.185	Gi0/1	192.168.1.239	11	0BD7	00A1	721
Gi0/0	10.89.16.226	Gi0/1	192.168.150.60	06	12CA	0016	127

router#

In the preceding example, there are several single packet flows for **TCP ports 139 (hex value 008B)** and **445 (hex value 01BD)** to sequential destination IP addresses. Administrators should compare these flows to baseline utilization for TCP ports 139 and 445 and also investigate the flows to determine whether they are the result of a worm scan.

To view only the traffic flows for **TCP ports 139 (hex value 008B)** and **445 (hex value 01BD)**, the command **show ip cache flow | include SrcIf|_06_.*(008B|01BD)** will display the related NetFlow records as shown here:

```
router#show ip cache flow | include SrcIf|_06_.*(008B|01BD)
```

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/1	192.0.2.2	Gi0/0	192.168.1.10	06	058A	01BD	1
Gi0/1	192.0.2.2	Gi0/0	192.168.1.20	06	058A	01BD	1
Gi0/1	192.0.2.2	Gi0/0	192.168.1.26	06	058A	01BD	1
Gi0/1	192.0.2.2	Gi0/0	192.168.1.27	06	058A	01BD	1
Gi0/1	192.0.2.2	Gi0/0	192.168.1.28	06	058A	01BD	1
Gi0/1	192.0.2.2	Gi0/0	192.168.1.71	06	058A	008B	1
Gi0/1	192.0.2.2	Gi0/0	192.168.1.76	06	058A	008B	1
Gi0/1	192.0.2.2	Gi0/0	192.168.1.77	06	058A	008B	1
Gi0/1	192.0.2.2	Gi0/0	192.168.1.74	06	058A	008B	1
Gi0/1	192.0.2.2	Gi0/0	192.168.1.75	06	058A	008B	1

router#

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 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 TCP packets on ports 139 and 445. In the following example, 192.168.1.0/24 is the network IP address space used by CIFS servers. The host at 192.168.100.1 is considered a trusted CIFS networking client that requires access to the CIFS servers through an affected WAE device that is configured for Edge Services, which use CIFS optimization. Note that neither the tACL source nor destination IP addresses are that of the affected Edge WAE device. The tACL is constructed to allow TCP port 139 and 445 traffic only between trusted CIFS servers and trusted CIFS networking clients, which should provide mitigation from worm-affected devices that actively scan random IP addresses. Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic.

Additional information about tACLs is available in [Transit Access Control Lists: Filtering at Your Edge](#).

```
!  
!-- Include any explicit permit statements for trusted sources  
!-- requiring access on the vulnerable ports  
!  
access-list Transit-ACL-Policy  
extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0 eq 139  
access-list Transit-ACL-Policy  
extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0 eq 445  
  
!  
!-- The following vulnerability-specific access control entries  
!-- (ACEs) can aid in identification of attacks  
!  
access-list Transit-ACL-Policy  
extended deny tcp any 192.168.1.0 255.255.255.0 eq 139  
access-list Transit-ACL-Policy  
extended deny tcp any 192.168.1.0 255.255.255.0 eq 445  
  
!  
!-- 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 interfaces in the ingress direction  
!  
access-group Transit-ACL-Policy in interface outside  
  
!
```

Mitigation: Anti-Spoof Protection Using Unicast RPF

Attackers can exploit the denial of service vulnerability in Cisco WAAS software using 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 IP source address. Administrators should not rely on Unicast RPF to provide 100 percent anti-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 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](#).

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 destined to TCP ports 139 and 445 that have been filtered. Administrators should investigate filtered packets to determine whether they are attempts to exploit this vulnerability. Example output for **show access-list Transit-ACL-Policy** follows:

```
firewall#show access-list Transit-ACL-Policy
access-list Transit-ACL-Policy; 5 elements
access-list Transit-ACL-Policy line 1
extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0
eq netbios-ssn (hitcnt=0) 0x189f48a3
access-list Transit-ACL-Policy line 2
extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0
eq 445 (hitcnt=0) 0x6a75413
access-list Transit-ACL-Policy line 3
extended deny tcp any 192.168.1.0 255.255.255.0
eq netbios-ssn (hitcnt=154) 0xcf95426a
access-list Transit-ACL-Policy line 4
extended deny tcp any 192.168.1.0 255.255.255.0
eq 445 (hitcnt=912) 0xa147104c
access-list Transit-ACL-Policy line 5
extended deny ip any any (hitcnt=0) 0xc797eb99
firewall#
```

In the preceding example, access list *Transit-ACL-Policy* has dropped **154 packets for TCP port 139** and **912 packets for TCP port 445** 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 in [Cisco Security Appliance System Log Message - 106023](#).

Information about configuring syslog for the Cisco ASA 5500 Series Adaptive Security Appliance or

the Cisco PIX 500 Series Security Appliance is available in [Configuring Logging on the Cisco Security Appliance](#). Information about configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is available in [Configuring Monitoring and Logging on the Cisco FWSM](#).

In the following example, the **show logging | grep *regex*** command extracts syslog messages from the logging buffer on the firewall. These messages provide additional information about denied packets that could indicate potential attempts to exploit the vulnerability described in this document. It is possible to use different regular expressions with the **grep** keyword to search for specific data in the logged messages.

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

```
firewall#show logging | grep 106023
Jun 20 2007 17:08:03 PIX-525a : %PIX-4-106023:
Deny tcp src outside:192.0.2.2/1286 dst
  inside:192.168.1.71/139 by access-group
  "Transit-ACL-Policy" [0xcf95426a, 0x0]
Jun 20 2007 17:08:03 PIX-525a : %PIX-4-106023:
Deny tcp src outside:192.0.2.2/1418 dst
  inside:192.168.1.72/139 by access-group
  "Transit-ACL-Policy" [0xcf95426a, 0x0]
Jun 20 2007 17:08:03 PIX-525a : %PIX-4-106023:
Deny tcp src outside:192.0.2.2/1354 dst
  inside:192.168.1.73/445 by access-group
  "Transit-ACL-Policy" [0xa147104c, 0x0]
firewall#
```

In the preceding example, the messages logged for the tACL *Transit-ACL-Policy* show **packets for TCP port 139 and 445** sent to the address block assigned to CIFS servers.

Additional information about syslog messages for ASA and PIX security appliances is available in [Cisco Security Appliance System Log Messages](#). Additional information about syslog messages for the FWSM is available in [Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages](#).

Identification: Anti-Spoof 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 potential attempts to exploit the vulnerability described in this document. It is possible to use different regular expressions with the **grep** keyword to search for specific data in the logged messages.

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

```
firewall#show logging | grep 106021
Jun 20 2007 17:04:56 PIX-525a : %PIX-1-106021:
Deny TCP reverse path check from 192.0.2.2 to 192.168.1.71 on interface outside
Jun 20 2007 17:04:56 PIX-525a : %PIX-1-106021:
Deny TCP reverse path check from 192.0.2.2 to 192.168.1.72 on interface outside
Jun 20 2007 17:04:56 PIX-525a : %PIX-1-106021:
Deny TCP reverse path check from 192.0.2.2 to 192.168.1.73 on interface outside
Jun 20 2007 17:04:57 PIX-525a : %PIX-1-106021:
Deny TCP reverse path check from 192.0.2.2 to 192.168.1.74 on interface outside
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                160
  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 **160 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: IPS Signature Event Actions

The Cisco Intrusion Prevention System (IPS) appliances and services modules can be used to provide threat detection and prevention against attempts to exploit the vulnerability described in this document. The vulnerability described in this document may be detected by three signatures:

- 6009 - SYN Flood DOS
- 3030 - TCP SYN Host Sweep
- 13003 - AD - External TCP Scanner

6009 - SYN Flood DOS

Starting with signature update S214 for sensors running Cisco IPS version 6.x or 5.x, the 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 a signature fidelity rating (SFR) of 85, and is configured with a default event action of **Produce Alert**. Signature 6009/0

fires when 100 or more TCP SYN packets per second are detected between the same source and destination IP addresses. For best detection and prevention of this vulnerability, the **Event Counter > Event Count Key** should be changed to **Attacker address and victim port**. Additionally, the **Alert Frequency > Summary Mode > Summary Key** should be changed to **Attacker address and victim port**. Firing of this signature may indicate an attempt to exploit the vulnerability described in this document.

3030 - TCP SYN Host Sweep

Starting with signature update S2 for sensors running Cisco IPS version 6.x or 5.x, the vulnerability described in this document can be detected by signature 3030 (Signature Name: TCP SYN Host Sweep). Signature 3030 is enabled by default, triggers an Information severity event, has an SFR of 85, and is configured with a default event action of **Produce Alert**. Signature 3030 fires when 15 or more unique TCP SYN packets are detected from a single source IP address to a number of different destination IP addresses. Firing of this signature may indicate an attempt to exploit the vulnerability described in this document.

13003 - AD - External TCP Scanner

Starting with signature update S262 for sensors running Cisco IPS version 6.x or 5.x, the vulnerability described in this document can be detected by signature 13003 (Signature Name: AD- External TCP Scanner). Signature 13003 is enabled by default, triggers a High severity event, has an SFR of 100, and is configured with a default event action of **Produce Alert**. Signature 13003 fires when a TCP scanner is detected scanning a set of destination IP addresses configured as zone **External**. If no other zone is configured, all destination IP addresses belong to the **External** zone. Firing of this signature may indicate an attempt to exploit the vulnerability described in this document.

Administrators can configure Cisco IPS sensors 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 denial of service vulnerability in Cisco WAAS software described in this document.

Because SYN-based exploits do not require a successful TCP three-way handshake, they can use spoofed source addresses. An attack that contains spoofed addresses may cause a configured event action to inadvertently deny traffic from trusted sources. Event actions that perform blocking through ACLs or the **shun** command are usually configured on sensors deployed in promiscuous mode.

Cisco IPS sensors are most effective when deployed in inline protection mode coupled 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 attempting to exploit this vulnerability. This is done through a default override that performs an event action of **Deny Attacker Inline** 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](#).

Cisco IPS 5.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 that can perform an event action for any signatures that are triggered and are calculated as a high-risk threat. Using the **Deny Attacker Inline** event action on sensors deployed in inline protection mode provides the most effective exploit prevention.

Identification: IPS Signature Events

Signature: 6009/0 SYN Flood DOS

IPS# **show events alert**

```
evIdsAlert: eventId=1166795198236312459 vendor=Cisco severity=medium
originator:
  hostId: R4-IPS4240a
  appName: sensorApp
  appInstanceId: 27495
time: June 22, 2007 6:18:33 PM UTC offset=-300 timeZone=CDT
signature: description=SYN Flood DOS id=6009 version=S214
  subsigId: 0
  sigDetails: SYN Flood DOS
  marsCategory: DoS/Host
  marsCategory: DoS/Network/TCP
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: 192.0.2.2 locality=OUT
    port: 1286
  target:
    addr: 192.168.1.52 locality=OUT
    port: 139
    os: idSource=unknown type=unknown relevance=relevant
triggerPacket:
000000 00 15 2B 1A 18 64 00 15 63 50 50 C0 08 00 45 00 ..+...d...cPP...E.
000010 00 28 68 E1 00 00 3F 06 90 10 C0 00 02 02 C0 A8 .(h...?.....
000020 00 34 05 06 00 8B 00 00 00 00 00 00 00 00 50 02 .4.....P.
000030 00 00 27 73 00 00 00 00 00 00 00 00 00 00 00 ...'s.....

riskRatingValue: 73 targetValueRating=medium attackRelevanceRating=relevant
threatRatingValue: 73
interface: ge0_0
protocol: tcp
```

Signature: 3030 - TCP SYN Host Sweep

IPS# **show events alert**

```
evIdsAlert: eventId=1183121654086791161 vendor=Cisco severity=informational
originator:
  hostId: R4-IPS4240a
  appName: sensorApp
  appInstanceId: 384
time: July 10, 2007 4:02:28 AM UTC offset=-300 timeZone=CDT
signature: description=TCP SYN Host Sweep id=3030 version=S2
  subsigId: 0
  marsCategory: Probe/SpecificPorts
interfaceGroup: vs1
vlan: 0
participants:
  attacker:
    addr: 192.0.2.2 locality=OUT
    port: 1418
  target:
```

```
    addr: 192.168.1.71 locality=OUT
    os: idSource=unknown type=unknown relevance=relevant
target:
    addr: 192.168.1.73 locality=OUT
    os: idSource=unknown type=unknown relevance=relevant
target:
    addr: 192.168.1.74 locality=OUT
    os: idSource=unknown type=unknown relevance=relevant
target:
    addr: 192.168.1.75 locality=OUT
    os: idSource=unknown type=unknown relevance=relevant
target:
    addr: 192.168.1.76 locality=OUT
    os: idSource=unknown type=unknown relevance=relevant
target:
    addr: 192.168.1.77 locality=OUT
    os: idSource=unknown type=unknown relevance=relevant
target:
    addr: 192.168.1.78 locality=OUT
    os: idSource=unknown type=unknown relevance=relevant
target:
    addr: 192.168.1.79 locality=OUT
    os: idSource=unknown type=unknown relevance=relevant
target:
    addr: 192.168.1.80 locality=OUT
    os: idSource=unknown type=unknown relevance=relevant
target:
    addr: 192.168.1.81 locality=OUT
    os: idSource=unknown type=unknown relevance=relevant
target:
    addr: 192.168.1.82 locality=OUT
    os: idSource=unknown type=unknown relevance=relevant
target:
    addr: 192.168.1.83 locality=OUT
    os: idSource=unknown type=unknown relevance=relevant
target:
    addr: 192.168.1.84 locality=OUT
    os: idSource=unknown type=unknown relevance=relevant
target:
    addr: 192.168.1.85 locality=OUT
    os: idSource=unknown type=unknown relevance=relevant
target:
    addr: 192.168.1.86 locality=OUT
    os: idSource=unknown type=unknown relevance=relevant
riskRatingValue: 31 targetValueRating=medium
attackRelevanceRating=relevant
threatRatingValue: 31
interface: ge0_1
protocol: tcp
```

Signature: 13003 - AD - External TCP Scanner

IPS# **show events alert**

```
evIdsAlert: eventId=1183121654086794947 vendor=Cisco severity=high
originator:
  hostId: R4-IPS4240a
  appName: sensorApp
  appInstanceId: 384
```

```
time: July 10, 2007 6:12:19 AM UTC offset=-300 timeZone=CDT
signature:  description=AD - External TCP Scanner id=13003 version=S262
  subsigId: 0
  sigDetails: Single Scanner
  marsCategory: Info/Misc/Scanner
  marsCategory: Probe/FromScanner
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: 192.168.0.2  locality=OUT
  target:
    addr: 0.0.0.0  locality=Unknown
    port: 445
actions:
  denyPacketRequestedNotPerformed: true
alertDetails: .  adExtraData: numDestIps=200; currentThreshold=200;
  destPort=445 ;
riskRatingValue: 100  targetValueRating=medium
threatRatingValue: 100
interface: sy0_0
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 vulnerability in Cisco WAAS software using a query type and keywords. Using keywords of **NR-6009/0** for IPS signature 6009/0, **NR-3030** for IPS signature 3030, and **NR-13003** for IPS signature 13003 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 6009/0, 3030, or 13003.

6009 - 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.

Cisco Systems

SUMMARY INCIDENTS QUERY / REPORTS RULES MANAGEMENT ADMIN HELP

Incidents | False Positives | Cases Jun 22, 2007 1:35:51 PM CDT

INCIDENTS | CS-MARS Standalone: R4-MARS v4.2 Log in: Administrator (psadmin) | Logout | Activate

View Cases New Case

Incident ID: 24599193 Show
Session ID: Show

Rule Name: System Rule: DoS: Network - Attempt Status: Active
Action: None Time Range: 0h:30m
Description: This rule detects network level denial of service (DoS) attacks along with relevant reconnaissance activity that may have preceded the attacks. Such attacks can create a dramatic increase in overall network traffic.

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/WI	ANY	None	ANY	ANY	1		FOLLOWED-BY
2		ANY	SAME, \$TARGET01, ANY	ANY	DoS/Network/TCP, DoS/Network/UDP, DoS/Network/ICMP, DoS/Network/PSs, DoS/Distributed	ANY	None	ANY	ANY	1]	OR
3		ANY	SAME, \$TARGET01, ANY	ANY	DoS/Network/TCP, DoS/Network/UDP, DoS/Network/ICMP, DoS/Network/PSs, DoS/Distributed	ANY	None	ANY	ANY	1		

Incident ID: 24599193 Expand All Collapse All

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	False Positive
3	S:33419510, 7:26599193, I:26599194	NSV-open SYN Attack / SYN Flood Denial of Service	192.0.2.2 1286	192.168.0.52 139	TCP	Jun 22, 2007 1:18:33 PM CDT	R4-IP54240			False Positive

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

Trusted sites

3030 - TCP SYN Host Sweep

Cisco Security MARS will create an incident if signature TCP SYN Host Sweep is triggered. This occurs when 15 or more unique TCP SYN packets are detected from a single source IP address to a number of different destination IP addresses. Signature 3030 triggers events for the Cisco Security MARS event type **TCP SYN Host Sweep On Same Dest Port**.

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

Rule Name: System Rule: Scans: Targeted Status: Active
 Action: None Time Range: 0h:10m
 Description: This rule detects scans that are either (a) targeted at a host to identify its operating environment, such as users on a host, DNS version, RPC services open etc. or (b) targeted at a well-known service to determine the set of host that offer that service.

Offset	Open (Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	Close	Operation
1	ANY	SAME, \$TARGET01, ANY	ANY	ANY	Probe/SpecifiPorts, Probe/Host/Config, Probe/Host/WinRegistry, Probe/Host/UserName, Probe/Host/NetworkShare, Probe/ServerInfo/DNS, Probe/ServerInfo/Mail, Probe/ServerInfo/FTP, Probe/ServerInfo/RPC, Probe/ServerInfo/DB, Probe/ServerInfo/Web, Probe/ServerInfo/Login, Probe/PromiscuousHost, Probe/Firewall, SAME, \$EVENT_TYPE01	SAME, \$DEVICE01	None	ANY	RED	1		OR
2	ANY	SAME, \$TARGET01, ANY	ANY	ANY	Probe/SpecifiPorts, Probe/Host/Config, Probe/Host/WinRegistry, Probe/Host/UserName, Probe/Host/NetworkShare, Probe/ServerInfo/DNS, Probe/ServerInfo/Mail, Probe/ServerInfo/FTP, Probe/ServerInfo/RPC, Probe/ServerInfo/DB, Probe/ServerInfo/Web, Probe/ServerInfo/Login, Probe/PromiscuousHost, Probe/Firewall, SAME, \$EVENT_TYPE01	SAME, \$DEVICE01	None	ANY	YELLOW	1		

Incident ID: 34362761 [Expand All](#) [Collapse All](#)

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	False Positive
Instance 1										
2		TCP SYN Host Sweep On Same Dest Port	192.168.0.2 1418	192.168.1.74 0	TCP	Jul 10, 2007 11:16:07 PM CDT	R4-IP54340a		Total: 2	
2	S:42517007, I:34362761	TCP SYN Host Sweep On Same Dest Port	192.168.0.2 1418	192.168.1.74 0	TCP	Jul 10, 2007 11:16:07 PM CDT	R4-IP54340a			False Positive
2	S:42517023, I:34362761	TCP SYN Host Sweep On Same Dest Port	192.168.0.2 1418	192.168.1.74 0	TCP	Jul 10, 2007 11:16:07 PM CDT	R4-IP54240a			False Positive

13003 - AD - External TCP Scanner

Cisco Security MARS will create an incident if signature AD- External TCP Scanner is triggered. This occurs when a TCP scanner is detected scanning a set of destination IP addresses configured as zone **External**. Signature 13003 triggers events for the Cisco Security MARS event type **Anomaly Detection - External TCP Scanner**.

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

Incidents | False Positives | Cases | Jul 10, 2007 1:06:45 AM CDT

INCIDENTS | CS-MARS Standalone: R4-MARS v4.2 | Login: Administrator (padmin) | Logout | Activate

View Cases | New Case

Incident ID: 34362618 | Show
Session ID: | Show

Rule Name: System Rule: Scans: Stealth, Copied: 07.03.12/23:31:59 | Status: Active
Action: None | Time Range: 0h:10m
Description: This rule detects highly suspicious scans that are performed by sending malformed TCP/IP packets with an intent to discover host and application characteristics such as OS name, OS version etc. A vulnerability assessment tool such as Nmap can generate such scans. The source of the scans, if from inside the trusted network, must be investigated to see if it is from an authorized source. A MARS appliance may be performing such a test as part of false positive analysis.

Offset	Open	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	Close	Operation
1		ANY	ANY	ANY	Probe:HostSweep/Stealth, Probe:PortSweep/Stealth, Probe:FromScanner, Probe:Host/Stealth	ANY	None	ANY	ANY	1		

Incident ID: 34362618 | Expand All | Collapse All

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	False Positive
1		Anomaly Detection - External TCP Scanner	192.168.0.2	0.0.0.0	445 TCP	Jul 10, 2007 12:47:32 AM CDT	R4-IP9420a		Total: 2	
1	S:4234569, I:34362618, I:34362618	Anomaly Detection - External TCP Scanner	192.168.0.2	0.0.0.0	445 TCP	Jul 10, 2007 12:47:32 AM CDT	R4-IP9420a			False Positive
1	S:4234569, I:34362618, I:34362618	Anomaly Detection - External TCP Scanner	192.168.0.2	0.0.0.0	445 TCP	Jul 10, 2007 12:47:32 AM CDT	R4-IP9420a			False Positive

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

The following screen shot shows the values used to query for events created by IPS Signature 6009/0 (Signature Name: SYN Flood DOS), IPS Signature 3030 (Signature Name: TCP SYN Host Sweep), or IPS Signature 13003 (Signature Name: AD- External TCP Scanner).

Query | Batch Query | Report | Jul 10, 2007 1:30:36 AM CDT

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

View Cases | New Case

Query Event Data
Click the cells below to change query criteria:

Query type: Event Types ranked by Sessions, 0h:10m | Edit | Clear

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-6009/0 OR NR-3030 OR NR-13003	None	ANY	ANY

Apply

Specify raw message keywords:

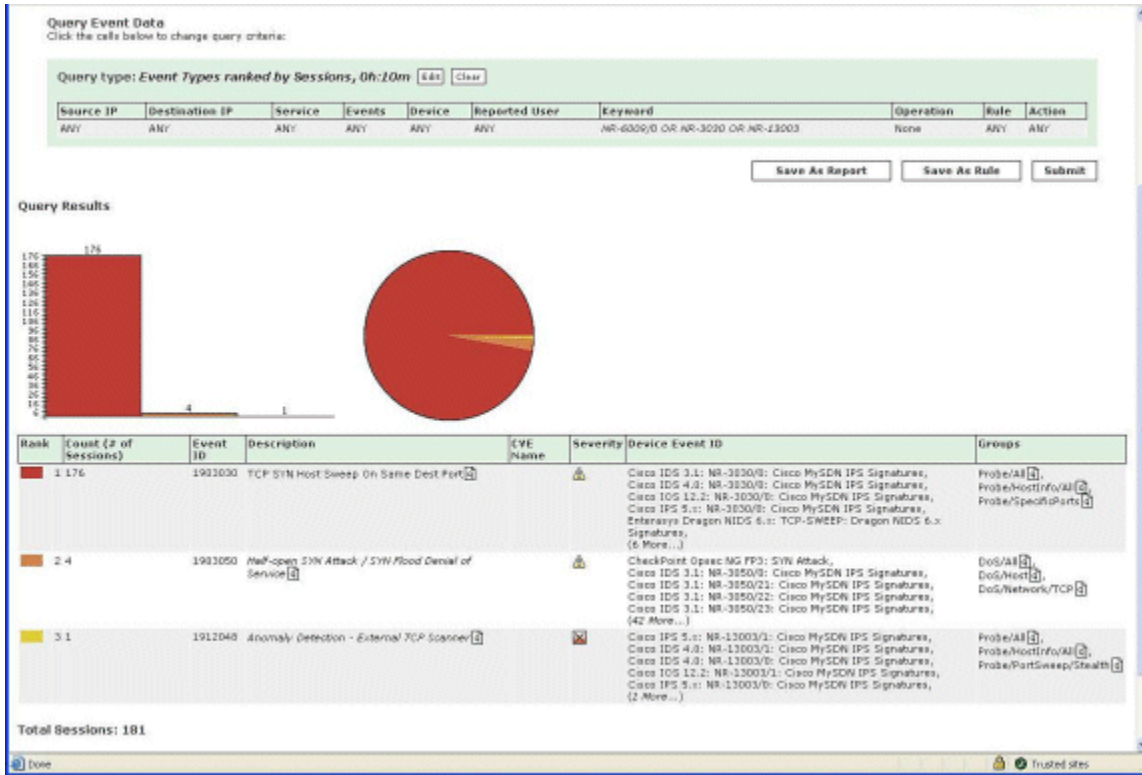
Open	Search String	Close	Operation	Highlight
	NR-6009/0		OR	
	NR-3030		OR	
	NR-13003		None	
			None	
			None	
			None	
			None	
			None	
			None	
			None	

Cancel | Apply

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

The following screen shot shows the query results for NR-6009/0, NR-3030, or NR-13003 created by

the Cisco Security MARS appliance using a query type and keyword regex query.



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-JUL-21	Added line breaks
Revision 1.0	2007-JUL-18	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/en/US/products/products_security_advisories_listing.html.

Related Information

- [Cisco Applied Mitigation Bulletins](#)
 - [Transit Access Control Lists: Filtering at Your Edge](#)
 - [Access Control List Logging](#)
 - [Unicast Reverse Path Forwarding](#)
 - [Cisco IOS NetFlow - Home Page on Cisco.com](#)
 - [Cisco IOS NetFlow White Papers](#)
 - [Cisco Network Foundation Protection White Papers](#)
 - [Cisco Network Foundation Protection Presentations](#)
 - [Cisco Firewall Products - Home Page on Cisco.com](#)
 - [Unicast Reverse Path Forwarding Loose Mode](#)
 - [Unicast Reverse Path Forwarding Enhancements for the Internet Service Provider - Internet Service Provider Network Edge](#)
 - [Cisco 6.x Intrusion Prevention System](#)
 - [Cisco IPS Risk Rating Explained](#)
 - [Cisco IPS 6.x Signature Downloads](#)
 - [Cisco IPS Signatures by Release Version](#)
 - [Cisco IPS Signatures by Signature ID](#)
 - [Cisco Security Monitoring, Analysis, and Response System](#)
 - [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](#)

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