

Cisco Applied Intelligence Response: Identifying and Mitigating Exploitation of the Microsoft Workstation Service Remote Buffer Overflow Vulnerability

Document ID: 72691

<http://www.cisco.com/warp/public/707/cisco-air-20061201-ms06-070-vulnerability.shtml>

Revision 1.0

For Public Release 2006 December 01 1600 UTC (GMT)

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

[Cisco Response](#)

[Cisco ASA, PIX, and FWSM Firewalls](#)

[Cisco Intrusion Prevention System \(IPS\)](#)

[Cisco Security Agent](#)

[Cisco VPN Termination Devices](#)

[Internet Edge Routers](#)

[Cisco Security Monitoring, Analysis, and Response System \(Cisco Security MARS\)](#)

[Additional Information](#)

[Revision History](#)

[Cisco Security Procedures](#)

[Related Information](#)

Cisco Response

Vulnerability Characteristics

Microsoft Windows "Workstation Service (wkssvc.dll)" contains a flaw that is vulnerable to a buffer overflow. When successfully exploited, this vulnerability allows remote code execution with SYSTEM privileges. Successful exploitation of this vulnerability could allow an attacker complete control of an affected system or create a denial-of-service (DoS) condition.

This vulnerability can be exploited remotely without authentication or user interaction. However, remote exploitation without authentication is limited to systems running Windows 2000 Service Pack 4. The attack vector is through TCP ports 139 (netbios-ssn) and 445 (microsoft-ds). This vulnerability is designated by CVE ID 2006-4691.

Vulnerability Overview

This document contains information to assist Cisco customers in mitigating attempts to exploit the Microsoft Workstation Service Could Allow Remote Code Execution vulnerability ([MS06-070](#)). An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Computers using the following operating systems are affected:

- Microsoft Windows 2000 Service Pack 4 (remotely exploitable with no authentication)
- Microsoft Windows XP Service Pack 2 (locally exploitable, requires a user with Administrator privileges)

Computers using the following operating systems are not affected:

- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 for Itanium-based Systems
- Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition
- Windows Vista

See the [Microsoft Security Bulletin MS06-070](#) for full details.

Mitigation Technique Overview

Cisco devices provide several countermeasures for the MS06-070 vulnerability. Cisco Security Agent provides the most preventive control at the end-host level. The Cisco Security Agent rule set that is enabled by default will mitigate attempts to exploit this vulnerability from all known attack vectors. The Cisco Intrusion Prevention System (IPS) product suite can perform detective or preventive controls using signatures 5822/0 or 5818/0. Administrators can reduce threat exposure using access lists applied on Cisco IOS Software and on Cisco Adaptive Security Appliance (ASA)/PIX Firewall Software/Firewall Services Module (FWSM) firewall products and using access controls applied to VPN connections.

One of the recommendations in this document is to filter IP traffic on TCP ports 139 (netbios-ssn) and 445 (microsoft-ds). It should be noted that multiple Windows services use these ports and blocking all connectivity to the ports may cause various applications or services to not function. Some of the applications or services that could be impacted are listed below.

- Applications that uses SMB (CIFS)
- Applications that uses mailslots or named pipes (RPC over SMB)
- Server (File and Print Sharing)
- Group Policy
- Net Logon
- Distributed File System (DFS)
- Terminal Server Licensing
- Print Spooler
- Computer Browser
- Remote Procedure Call Locator
- Fax Service
- Indexing Service
- Performance Logs and Alerts
- Systems Management Server
- License Logging Service

The effectiveness of any mitigation technique depends on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Because a variety of products and releases are affected, customers should consult with their service providers or support organizations to ensure that any workaround is the most appropriate for use in the intended network before it is deployed.

General Worm Mitigation

For general information regarding strategies and technologies for worm mitigation, refer to [Worm Mitigation Technical Details](#).

Device-Specific Mitigation and Identification

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

- [Cisco ASA, PIX, and FWSM Firewalls](#)
- [Cisco Intrusion Prevention System \(IPS\)](#)
- [Cisco Security Agent](#)
- [Cisco VPN Termination Points](#)
- [Internet Edge Routers](#)
- [Cisco Security Monitoring, Analysis, and Response System \(Cisco Security MARS\)](#)

Cisco ASA, PIX, and FWSM Firewalls

PIX/ASA 7.x



Caution: As with any configuration change in a network, evaluate the impact of this configuration prior to applying the change.

Mitigation

Firewall access-control lists (ACLs) can limit access to devices affected by the MS06-070 vulnerability. The following ACL is designed to deny access to internal hosts on TCP ports 139 (netbios-ssn) and 445 (microsoft-ds). It can be applied inbound on the outside interface of a PIX/ASA firewall running 7.x software to prevent the spread of the MS06-070 exploit on the network:

```
!-- MS06-070 - Block initial scanning on Internet-facing interfaces.  
!-- Note: When blocking TCP/139 (netbios-ssn) and TCP/445 (microsoft-ds),  
!-- take care to ensure that legitimate connections are not impacted.  
  
access-list ms06-070-in extended deny tcp any any eq netbios-ssn  
access-list ms06-070-in extended deny tcp any any eq 445  
  
!-- Permit/deny other IP traffic in accordance with existing security policy.  
  
!  
access-group ms06-070-in in interface outside
```

Identification

The following example displays the output for the **show access-list ms06-070-in** command. In the example, 150 packets bound for TCP port 139 (netbios-ssn) and 55 packets bound for TCP port 445 (microsoft-ds) have been dropped by the ACL configured inbound on the outside interface. These packets may be an attempt to exploit the MS06-070 vulnerability and should be investigated.

```
ASA5520a#show access-list ms06-070-in  
access-list ms06-070-in; 2 elements  
access-list ms06-070-in line 1 extended deny tcp any any eq netbios-ssn (hitcnt=150)  
access-list ms06-070-in line 2 extended deny tcp any any eq 445 (hitcnt=55)
```

A syslog warning level (level 4) message, 106023, is generated when a firewall ACL drops packets as shown by these examples:

```
Nov 17 2006 17:44:27: %ASA-4-106023: Deny tcp src outside:10.89.236.135/1286
dst inside:192.168.0.1/139 by access-group "ms06-070-in"
```

```
Nov 17 2006 17:45:57: %ASA-4-106023: Deny tcp src outside:10.89.236.135/1286
dst inside:192.168.0.1/445 by access-group "ms06-070-in"
```

For more information, refer to [Cisco Security Appliance System Log Message 106023](#).

FWSM



Caution: As with any configuration change in a network, evaluate the impact of this configuration prior to applying the change.

Mitigation

Firewall ACLs can limit access to devices affected by the MS06-070 vulnerability. The following ACL is designed to deny access to internal hosts on TCP ports 139 (netbios-ssn) and 445 (microsoft-ds). It can be applied inbound on the outside interface of a FWSM to prevent the spread of the MS06-070 exploit on customer networks:

```
!-- MS06-070 - Block initial scanning on Internet-facing interfaces.
!-- Note: When blocking TCP/139 (netbios-ssn) and TCP/445 (microsoft-ds),
!-- take care to ensure that legitimate connections are not impacted.

access-list ms06-070-in extended deny tcp any any eq netbios-ssn
access-list ms06-070-in extended deny tcp any any eq 445

!-- Permit/deny other IP traffic in accordance with existing security policy.

!
access-group ms06-070-in in interface outside
```

Identification

The following is an example of output for the **show access-list ms06-070-in** command. In the example, 115 packets bound for TCP port 139 (netbios-ssn) and 233 packets bound for TCP port 445 (microsoft-ds) have been dropped by the ACL configured inbound on the interface outside. These packets may be an attempt to exploit the MS06-070 vulnerability and should be investigated.

```
FWSM#show access-list ms06-070-in
access-list ms06-070-in; 2 elements
access-list ms06-070-in line 1 extended deny tcp any any eq netbios-ssn (hitcnt=115)
access-list ms06-070-in line 2 extended deny tcp any any eq 445 (hitcnt=233)
```

A syslog warning level (level 4) message, 106023, is generated when a FWSM ACL drops packets as shown by these examples:

```
Nov 17 2006 17:44:27: %FWSM-4-106023: Deny tcp src outside:10.89.236.135/1286
dst inside:192.168.0.1/139 by access-group "ms06-070-in"
```

```
Nov 17 2006 17:45:57: %FWSM-4-106023: Deny tcp src outside:10.89.236.135/1286
dst inside:192.168.0.1/445 by access-group "ms06-070-in"
```

For more information, refer to [Cisco FWSM System Log Message 106023](#).

Cisco Intrusion Prevention System (IPS)

Mitigation

The Cisco Intrusion Prevention System (IPS) can detect attempted exploitation of the MS06–070 vulnerability starting with signature update S255 for 5.x devices. This is achieved through signatures 5818/0 (S255) and 5822/0 – 5822/2 (S259). Signature 5818/0 is enabled by default and is triggered upon detecting attempts to exploit the Windows Workstation Service using exploit code that is publicly available.

Note: Signatures 5822/0 – 5822/2 were released as part of Signature Update S259, but these signatures are not triggered by public exploit code for MS06–070 at the time this document is being published. Signatures 5822/0 – 5822/2 could only be triggered using internal exploit code that is not currently available to the public.

Identification

IPS signature 5818/0 triggers a Medium severity alarm on potential attempts to exploit the Windows Workstation Service vulnerability which may indicate a remote code execution attack.

The following event was triggered by signature 5818/0 after a potential attempt to exploit the Windows Workstation Service on the target victim at IP address 192.168.130.121.

```
IDSM2#show events alert | include id=5818

evIdsAlert: eventId=1164166875640207141 severity=medium vendor=Cisco
  originator:
    hostId: IDSM2
    appName: sensorApp
    appInstanceId: 3861
  time: 2006/11/28 22:30:26 2006/11/28 16:30:26 CST
  signature: description=Metasploit Shellcode Encoder id=5818 version=S256
    subsigId: 0
    sigDetails: PexFnstenv Encoder
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.208.63
      port: 2352
    target:
      addr: locality=OUT 192.168.130.121
      port: 445
  context:
    fromAttacker:
/--- Output Truncated---
```

Cisco Security Agent

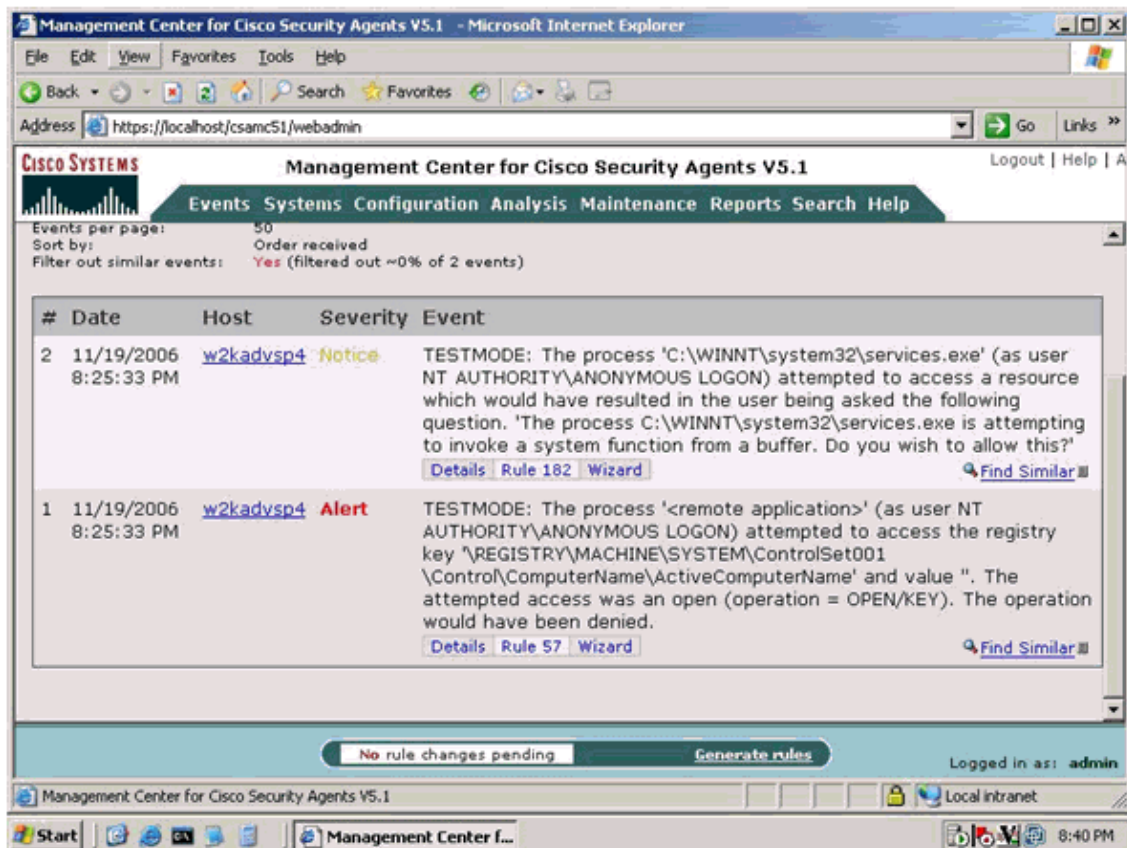
Mitigation

Cisco Security Agent provides mitigation through buffer overflow protection mechanisms that prevent the exploit from doing damage. These mechanisms are part of the default rule set and are enabled by default (i.e., no updates to the Cisco Security Agent software and/or the default rule set are required). Current supported versions of Cisco Security Agent 4.5.x, 5.0.x, and 5.1.x are all effective in stopping the exploits seen to date. The Cisco Security Agent agents must be set in Protect Mode (not Test Mode) to prevent this exploit.

Identification

As shown in the following example, the Cisco Security Agent Management Center console can be monitored for attempts to exploit this vulnerability.

Note: In the following example, Cisco Security Agent is configured in "Test Mode" in order to display all of the possible ways that the Cisco Security Agent default policies would stop the MS06-070 exploit. When the agent is in protect mode (the typical operational configuration), the first rule would stop the exploit and no subsequent events would be seen, since the exploit would be terminated before it could perform any malicious actions.




The screenshot shows the Management Center for Cisco Security Agents V5.1 interface. The main content area displays a table of events:

#	Date	Host	Severity	Event
2	11/19/2006 8:25:33 PM	w2kadvsp4	Notice	TESTMODE: The process 'C:\WINNT\system32\services.exe' (as user NT AUTHORITY\ANONYMOUS LOGON) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\WINNT\system32\services.exe is attempting to invoke a system function from a buffer. Do you wish to allow this?' Details Rule 182 Wizard Find Similar
1	11/19/2006 8:25:33 PM	w2kadvsp4	Alert	TESTMODE: The process '<remote application>' (as user NT AUTHORITY\ANONYMOUS LOGON) attempted to access the registry key '\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName' and value ". The attempted access was an open (operation = OPEN/KEY). The operation would have been denied. Details Rule 57 Wizard Find Similar

At the bottom of the interface, a status bar indicates "No rule changes pending" and "Generate rules". The user is logged in as "admin".

Cisco VPN Termination Devices

 **Caution:** As with any configuration change in a network, evaluate the impact of this configuration prior to applying the change.

Mitigation

Access control on site-to-site VPNs should provide users access to only those resources that they need rather than using an implicit trust model. Therefore, applying an ACL to block TCP ports 139 (netbios-ssn) and 445 (microsoft-ds) as part of standard VPN configurations is recommended unless business use dictates otherwise. The "Network Ingress Inbound Filtering" example provides a sample IOS ACL that could be applied to the decrypted VPN traffic as it exits the VPN termination device or be applied to another screening device that is located at the next hop from the VPN termination device.

Any added ACL entries should be implemented as part of a transit ACL that filters transit and edge traffic at network ingress points. For more information about transit ACLs, refer to [Transit Access Control Lists](#):

[Filtering at Your Edge.](#)

Note: If you are trying to track source addresses, use Sampled NetFlow, rather than **log** statements in access lists because the high traffic in combination with the **log** statement can overwhelm the router. The command **show access-list** can be used to determine the hit count against individual access list entries. This data can be used in conjunction with Sampled NetFlow to determine which specific worm variants (if any) are attacking the network.

Network Ingress Inbound Filtering

```
!-- MS06-070 - Block initial scanning on Internet-facing interfaces
!-- Note: When blocking TCP/139 (netbios-ssn) and TCP/445 (microsoft-ds),
!-- take care to ensure that legitimate connections are not impacted.

access-list 101 deny tcp any any eq 445
access-list 101 deny tcp any any eq 139

!-- Permit/deny other IP traffic in accordance with existing security policy.

!
interface serial 2/0
ip access-group 101 in
!
```

Identification

With a transit ACL, after interface access list 101 is deployed, the command **show access-list 101** can be used to identify the number of packets being dropped. Dropped packets should be investigated to determine if they are attempts to exploit the issue.

```
Edge-Router#show access-list 101
Extended IP access list 101
10 deny tcp any any eq 445 (141 matches)
20 deny tcp any any eq 139 (100 matches)
```

In the above example, 100 packets bound for TCP port 139 (netbios-ssn) and 141 packets bound for TCP port 445 (microsoft-ds) have been dropped by the ACL configured inbound on interface serial 2/0.

Internet Edge Routers



Caution: As with any configuration change in a network, evaluate the impact of this configuration prior to applying the change.

Mitigation

Transit ACLs allow administrators to configure Cisco IOS routers with interface ACLs to drop packets that could be used to exploit this issue.

Any added ACL entries should be implemented as part of a transit ACL that filters transit and edge traffic at network ingress points. For more information on transit ACLs, refer to [Transit Access Control Lists: Filtering at Your Edge.](#)

Note: If you are trying to track source addresses, use Sampled NetFlow, rather than **log** statements in access lists because the high traffic in combination with the **log** statement can overwhelm the router and possibly

result in high CPU utilization. The command **show access-list** can be used to determine the hit count against individual access-list entries. This data can be used in conjunction with Sampled NetFlow to determine which specific worm variants (if any) are attacking the network.

```
!-- MS06-070 - Block initial scanning on Internet-facing interfaces
!-- Note: When blocking TCP/139 (netbios-ssn) and TCP/445 (microsoft-ds),
!-- take care to ensure that legitimate connections are not impacted.

access-list 101 deny tcp any any eq 445
access-list 101 deny tcp any any eq 139

!-- Permit/deny other IP traffic in accordance with existing security policy.

!
interface serial 2/0
ip access-group 101 in
!
```

Please note that filtering traffic with an interface access list will cause ICMP unreachable messages to be transmitted back to the source of the filtered traffic. This could have the undesired side effect of high CPU utilization while the device generates these ICMP unreachable messages. In Cisco IOS Software, ICMP unreachable generation is limited to one packet per 500 ms. ICMP unreachable generation can be disabled using the interface configuration command **no ip unreachable**. ICMP unreachable rate limiting can be changed from the default of 1 per 500 ms using the global configuration command **ip icmp rate-limit unreachable (milliseconds)**. Millisecond values in the range of 1 through 4294967295 will be accepted.

Note: When filtering at the Port level (e.g. TCP/139/netbios-ssn or TCP/445/microsoft-ds), the ICMP type/code messages sent by the IOS device will be type 3 (destination unreachable)/code 3 (port unreachable).

Identification

With a transit ACL, after an interface access list 101 is deployed, the command **show access-list 101** can be used to identify the number of packets being dropped. Dropped packets should be investigated to determine if they are attempts to exploit the issue.

```
Edge-Router#show access-list 101
Extended IP access list 101
10 deny tcp any any eq 445 (141 matches)
20 deny tcp any any eq 139 (100 matches)
```

In the above example, 100 packets bound for TCP port 139 (netbios-ssn) and 141 packets bound for TCP port 445 (microsoft-ds) have been dropped by the ACL configured inbound on interface serial 2/0.

NetFlow

NetFlow can be configured on Internet edge routers and VPN termination routers to determine if attempts to exploit this vulnerability are in progress.

```
R1-6509Ea#show ip cache flow

-----
MSFC:
IP packet size distribution (36621 total packets):
1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
.407  .259  .308  .005  .001  .000  .000  .017  .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, 4456704 bytes
 33 active, 65503 inactive, 17877 added
140689 aged polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds

```

```

IP Sub Flow Cache, 270664 bytes
 33 active, 16351 inactive, 17877 added, 17877 added to flow
 0 alloc failures, 0 force free
 1 chunk, 1 chunk added
last clearing of statistics never

```

Protocol	Total	Flows	Packets	Bytes	Packets	Active(Sec)	Idle(Sec)
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
TCP-Telnet	88	0.0	101	41	0.0	18.8	14.3
TCP-FTP	3	0.0	1	40	0.0	0.0	15.4
TCP-WWW	7	0.0	2	124	0.0	0.0	9.6
TCP-SMTP	3	0.0	1	40	0.0	0.0	15.4
TCP-other	180	0.0	1	43	0.0	0.0	15.0
UDP-DNS	13732	0.0	1	28	0.0	0.5	18.5
UDP-NTP	2	0.0	1	76	0.0	0.0	15.4
UDP-other	2185	0.0	4	88	0.0	11.0	15.5
ICMP	1639	0.0	1	82	0.0	0.0	15.4
IP-other	5	0.0	47	131	0.0	222.2	15.4
Total:	17844	0.0	2	51	0.0	1.9	17.8

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Vl1000	10.88.226.3	Null	224.0.0.10	58	0000	0000	166
Vl2	10.89.236.132	Local	10.89.236.151	06	0791	008B	1
Vl2	10.89.236.132	Local	10.89.236.151	06	07D2	008B	1
Vl2	10.89.236.132	Local	10.89.236.151	06	0738	008B	1
Vl2	10.89.236.132	Local	10.89.236.151	06	0704	008B	1
Vl2	10.89.236.132	Local	10.89.236.151	06	0760	008B	1
Vl2	10.89.236.132	Local	10.89.236.151	06	06A0	008B	1
Vl2	10.89.236.132	Local	10.89.236.151	06	06B9	008B	1
Vl2	10.89.236.132	Local	10.89.236.151	06	06D5	008B	1
Vl2	10.89.236.132	Local	10.89.236.151	06	061F	008B	1
Vl2	10.89.236.132	Local	10.89.236.151	06	0663	008B	1
Vl2	10.89.236.132	Local	10.89.236.151	06	067D	008B	1
Vl2	10.89.236.132	Local	10.89.236.151	06	0672	008B	1
Vl2	10.89.236.132	Local	10.89.236.151	06	06B0	01BD	1
Vl2	10.89.236.132	Local	10.89.236.152	06	06A9	01BD	1
Vl2	10.89.236.132	Local	10.89.236.153	06	06FE	01BD	1
Vl2	10.89.236.132	Local	10.89.236.154	06	06F0	01BD	1
Vl2	10.89.236.132	Local	10.89.236.155	06	06F4	01BD	1
Vl2	10.89.236.132	Local	10.89.236.156	06	0609	01BD	1
Vl2	10.89.236.132	Local	10.89.236.157	06	0600	01BD	1
Vl2	10.89.236.132	Local	10.89.236.158	06	0603	01BD	1
Vl2	10.89.236.132	Local	10.89.236.159	06	07A7	01BD	1

----- Output Truncated -----

In the above example, there are a very high number of flows on TCP port 139 (Hex 008B) and TCP port 445 (Hex 01BD) from a single IP address to multiple destination IP addresses. On Internet edge routers and potentially on VPN termination routers, this activity may indicate an attempt to exploit this vulnerability and should be compared to baseline utilization of these ports on the monitoring devices.

To view only the flows on TCP port 139 (Hex 008B) and TCP port 445 (Hex 01BD), the command **show ip cache flow | include SrcIf|008B|01BD** may be used as shown here:

```

R1-6509Ea#show ip cache flow | include SrcIf|008B|01BD

```

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Vl2	10.89.236.132	Local	10.89.236.151	06	0791	008B	1
Vl2	10.89.236.132	Local	10.89.236.152	06	07D2	008B	1
Vl2	10.89.236.132	Local	10.89.236.153	06	0738	008B	1
Vl2	10.89.236.132	Local	10.89.236.155	06	0704	008B	1

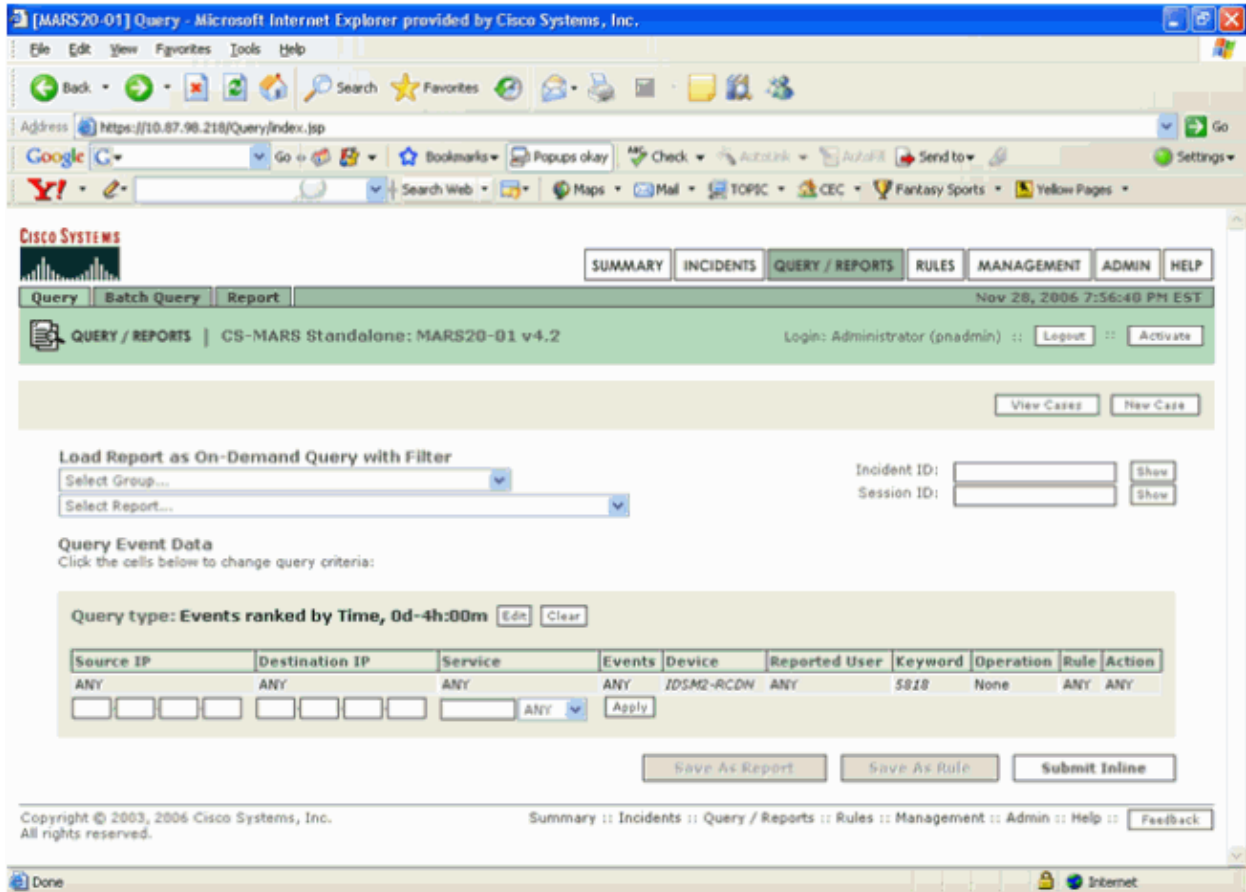
V12	10.89.236.132	Local	10.89.236.156	06 0760 008B	1
V12	10.89.236.132	Local	10.89.236.157	06 06A0 008B	1
V12	10.89.236.132	Local	10.89.236.158	06 06B9 008B	1
V12	10.89.236.132	Local	10.89.236.159	06 06D5 008B	1
V12	10.89.236.132	Local	10.89.236.160	06 061F 008B	1
V12	10.89.236.132	Local	10.89.236.161	06 0663 008B	1
V12	10.89.236.132	Local	10.89.236.162	06 067D 008B	1
V12	10.89.236.132	Local	10.89.236.163	06 0672 008B	1
V12	10.89.236.132	Local	10.89.236.164	06 0641 008B	1
V12	10.89.236.132	Local	10.89.236.165	06 065F 008B	1
V12	10.89.236.132	Local	10.89.236.151	06 06B8 01BD	1
V12	10.89.236.132	Local	10.89.236.152	06 06A5 01BD	1
V12	10.89.236.132	Local	10.89.236.153	06 06D9 01BD	1
V12	10.89.236.132	Local	10.89.236.154	06 06DA 01BD	1
V12	10.89.236.132	Local	10.89.236.155	06 06CC 01BD	1
V12	10.89.236.132	Local	10.89.236.156	06 06C6 01BD	1
V12	10.89.236.132	Local	10.89.236.157	06 0611 01BD	1
V12	10.89.236.132	Local	10.89.236.158	06 0630 01BD	1
V12	10.89.236.132	Local	10.89.236.159	06 0631 01BD	1
V12	10.89.236.132	Local	10.89.236.160	06 0677 01BD	1

----- Output Truncated -----

Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS)

Identification

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) console can be monitored for attempts to exploit the MS06-070 vulnerability. Using the following query on the Cisco Security MARS appliance, events triggered by signature 5818/0 will be displayed:



The display shown below is the result of the previous query for IPS events triggered by signature 5818/0:

Load Report as On-Demand Query with Filter

Incident ID: Show

Session ID: Show

Query Event Data

Click the cells below to change query criteria:

Query type: Events ranked by Time, 0d-4h:00m

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	IDSM2-RCDN	ANY	5818	None	ANY	ANY

Query Results

Event / Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Path / Mitigation	Tune
E:1189568468, S:1189568468	Unknown Device Event Type	192.168.208.63 2352	192.168.130.121 445	TCP	Nov 28, 2006 5:52:13 PM EST	IDSM2-RCDN		False Positive
E:1189557511, S:1189557511	Unknown Device Event Type	192.168.208.63 2352	192.168.130.121 139	TCP	Nov 28, 2006 5:40:29 PM EST	IDSM2-RCDN		False Positive
E:1189547839, S:1189547839	Unknown Device Event Type	192.168.208.63 1348	192.168.130.121 445	TCP	Nov 28, 2006 5:30:28 PM EST	IDSM2-RCDN		False Positive
E:1189547835, S:1189547835	Unknown Device Event Type	192.168.208.63 2352	192.168.130.121 445	TCP	Nov 28, 2006 5:30:26 PM EST	IDSM2-RCDN		False Positive

1 to 4 of 4 25 per page

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	2006-December-01	Initial public release.
--------------	------------------	-------------------------

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

Related Information

- [IPS 5.x Signature Downloads](#) ([registered](#) customers only)

- [Signatures by Release Version](#) ([registered](#) customers only)
 - [MySDN Report ID – 5228](#) ([registered](#) customers only)
 - [Microsoft Security Bulletin MS06–070](#)
 - [Microsoft Security Advisory \(928604\): Exploit Code Published Affecting the Workstation Service on Windows 2000](#)
 - [Cisco Systems IntelliShield Vulnerability Alert](#) (IntelliShield customers only)
 - [US–CERT Vulnerability Note VU#778036](#)
-

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

Updated: Dec 01, 2006

Document ID: 72691
