

# Cisco Security Response: Mitigating Exploitation of the MS06-040 Service Buffer Vulnerability

Document ID: 70997

<http://www.cisco.com/warp/public/707/cisco-sr-20060814-ms06-040>

## Revision 1.1

Last Updated 2006 August 21 2000 UTC (GMT)

For Public Release 2006 August 14 2300 UTC (GMT)

---

Please provide your feedback on this document.

---

**Cisco Response**  
**Cisco ASA and PIX Firewalls**  
**Cisco Intrusion Prevention System (IPS)**  
**Cisco Security Agent (CSA)**  
**Cisco VPN Termination Points**  
**Interface Access-lists**  
**NetFlow**  
**Additional Information**  
**Revision History**  
**Cisco Security Procedures**  
**Related Information**

---

## Cisco Response

### Vulnerability Characteristics

This vulnerability can be exploited remotely with no authentication and no user interaction necessary. If exploited, the attacker may perform remote code execution with the privileges of System or may create a Denial of Service. The attack vector is through TCP ports 139 and 445. This vulnerability is designated by CVE ID 2006-3439.

### Vulnerability Overview

This document contains information to assist Cisco customers in mitigating attempts to exploit the Microsoft Server Service Buffer Overflow Vulnerability. There is a remote code execution vulnerability in Server Service that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

Computers using the following operating systems are affected:

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1

- Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003
- 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

See MS06-040 for details of Windows platforms affected.

## Mitigation Technique Overview

Cisco devices provide several countermeasures for the MS06-040 vulnerability. The most preventative control is provided by Cisco Security Agent (CSA) at the end host level. The CSA default enabled rule set provides threat mitigation from all known attack vectors. Detective controls can be performed by the Cisco IPS product suite, which provides identification and protection starting with signature pack S243 using signatures 5799/0-5799/7. Access Lists applied on Cisco IOS® software, PIX, and ASA along with Access controls applied to VPN connections provide deterrents, thus reducing threat exposure.

The effectiveness of any mitigation technique is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied 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, please refer to the Cisco MySDN site at <http://www.cisco.com/web/about/security/intelligence/worm-mitigation-whitepaper.html>.

## Cisco ASA and PIX Firewalls

### PIX 6.x



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

The access list entries shown below include an example for one of the worm variants now being tracked. New variants using different ports are possible and should be filtered using the information below as examples.

The following access-list can be applied to a PIX Firewall running 6.x software to prevent/contain the spread of the MS06-040 exploit on customer networks.

### PIX 6.x: Network Ingress Inbound Filtering

```
!-- MS06-040 - Block Initial Scanning On Internet-facing Interfaces
!-- Note: When blocking TCP/139 and TCP/445, take care
!-- to ensure that legitimate connections are not impacted.

access-list ms06-040-in deny tcp any any eq netbios-ssn
access-list ms06-040-in deny tcp any any eq 445
```

```

!-- Block IRCBot.ST (aka W32.Wargbot, IRC-Mocbot!MS06-040,
!-- W32/Cuebot-L, Backdoor.Win32.IRCBot.st, WORM_IRCBOT.JL) IRC Creation
!-- in the event internal hosts have been compromised as a C&C bot.

access-list ms06-040-in deny tcp any any eq 18067

!-- Permit other traffic here.

access-list ms06-040-in permit ip any any

access-group ms06-040-in in interface outside

```

## PIX 6.x: Network Ingress Outbound Filtering

```

!-- MS06-040 - Block Initial Scanning By Infected Hosts

access-list ms06-040-out deny tcp any any eq netbios-ssn
access-list ms06-040-out deny tcp any any eq 445

!-- Block IRCBot.ST (aka W32.Wargbot, IRC-Mocbot!MS06-040,
!-- W32/Cuebot-L, Backdoor.Win32.IRCBot.st, WORM_IRCBOT.JL) IRC Creation
!-- in the event internal hosts have been compromised as a C&C bot.

access-list ms06-040-out deny tcp any any eq 18067

!-- Permit other traffic here.

access-list ms06-040-out permit ip any any

access-group ms06-040-out in interface inside

```

## PIX/ASA 7.x



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

The access list entries shown below include an example for one of the worm variants now being tracked. New variants using different ports are possible and should be filtered using the information below as examples.

The following access-list can be applied inbound to a PIX/ASA Firewall running 7.x software to prevent/contain the spread of the MS06-040 exploit on customer networks:

### PIX/ASA 7.x: Network Ingress Inbound Filtering

```

!-- MS06-040 - Block Initial Scanning On Internet-facing Interfaces
!-- Note: When blocking TCP/139 and TCP/445, take care
!-- to ensure that legitimate connections are not impacted.

access-list ms06-040-in extended deny tcp any any eq netbios-ssn
access-list ms06-040-in extended deny tcp any any eq 445

!-- Block IRCBot.ST (aka W32.Wargbot, IRC-Mocbot!MS06-040,
!-- W32/Cuebot-L, Backdoor.Win32.IRCBot.st, WORM_IRCBOT.JL) IRC Creation
!-- in the event internal hosts have been compromised as a C&C bot.

```

```

access-list ms06-040-in extended deny tcp any any eq 18067

!-- Permit other traffic here.

access-list ms06-040-in extended permit ip any any

access-group ms06-040-in in interface outside

```

## PIX/ASA 7.x: Network Ingress Outbound Filtering

```

!-- MS06-040 - Block Initial Scanning By Infected Hosts

access-list ms06-040-out extended deny tcp any any eq netbios-ssn
access-list ms06-040-out extended deny tcp any any eq 445

!-- Block IRCBot.ST (aka W32.Wargbot, IRC-Mocbot!MS06-040,
!-- W32/Cuebot-L, Backdoor.Win32.IRCBot.st, WORM_IRCBOT.JL) IRC Creation
!-- in the event internal hosts have been compromised as a C&C bot.

access-list ms06-040-out extended deny tcp any any eq 18067

!-- Permit other traffic here.

access-list ms06-040-out extended permit ip any any

access-group ms06-040-out in interface inside

```

## Cisco Intrusion Prevention System (IPS)

### Mitigation

The Cisco Intrusion Prevention System (IPS) can provide detection of the MS06-040 vulnerability starting with signature pack S243 for 5.x devices.

- Signature Pack S243
  - ◆ Added signatures 5799/0 – 5799/6
- Signature Pack S244
  - ◆ Added meta signature 5799/7
  - ◆ Modified signature 5799/2
  - ◆ Retired signatures 5799/0 and 5799/3
- Signature Pack S245
  - ◆ Added signature 6013/0 for detection of DNS requests for the C&C channel of the WORM\_IRCBOT.JK botnet network
  - ◆ Modified signatures 5799/4 and 5799/7

The Cisco Intrusion Detection System (IDS) can provide detection of the MS06-040 vulnerability starting with signature pack S245 for 4.x devices.

- Signature Pack S245
  - ◆ Added signature 5799/0 (disabled by default)
  - ◆ Added signature 6013/0 for detection of DNS requests for the C&C channel of the WORM\_IRCBOT.JK botnet network

In order to trigger preventative controls, the IPS 5.x signatures 5799/4 and 5799/7 or the IDS 4.x signature 5799/0 will need to be configured to perform a response action. The actions that provide this type of mitigation are more effective when using an IPS device that is deployed in inline mode. This threat is TCP based so attacks are unlikely to be spoofed.

## Identification

IPS meta signatures 5799/4 and 5799/7 trigger a High severity alarm on potential exploits of the Windows Server Service vulnerability which may indicate a remote code execution attack. Supporting component signatures are used to detect the intermediate steps of the attack.

The following event was triggered by signature 5799/7 after a potential exploit of the Windows Server Service was attempted on the target victim at IP address 192.0.2.157.

```
evIdsAlert: eventId=1154989166673222106 severity=high vendor=Cisco
  originator:
  hostId: IDSM2
  appName: sensorApp
  appInstanceId: 2972
  time: 2006/08/10 17:41:10 2006/08/10 17:41:10 UTC
  signature: description=Server Service Code Execution id=5799 version=S244
    subsigId: 7
  sigDetails: Server Service Code Execution
  interfaceGroup:
  vlan: 0
  participants:
  attacker:
  addr: locality=OUT 192.0.2.157
  <TriggerPacket removed>
  riskRatingValue: 75
  interface: ge0_7
  protocol: IP protocol 0
```

## Signature Summary

A number of signatures were defined in signature packs S243, S244 and S245. Of these signatures, IPS 5.x customers should monitor for signatures 5799/4, 5799/7 and 6013/0 and IDS 4.x customers should monitor for 5799/0 and 6013/0. The rest of the IPS 5.x 5799/x signatures are components to identify individual steps in the attack. Signatures 5799/0 and 5799/3 are retired as of Signature Pack S244.

In addition, signature 11203/0 (Severity: MEDIUM, Enabled by default) can be modified to detect potential IRC bot activity on TCP port 18067 and 22522. Adding TCP 18067 and 22522 to the service-ports (TCP ports 6666, 6667, 6668 are already configured by default) used by Signature 11203/0 can be done as follows:

### IPS 5.x Sig 11203/0 Modification Example

```
IPS#config t
IPS(config)#service signature-definition sig0
IPS(config-sig)#signatures 11203 0
IPS(config-sig-sig)#engine string-tcp
IPS(config-sig-sig-str)#service-ports 6666-6666,6667-6667,6668-6668,18067-18067,22522-22522
IPS(config-sig-sig-str)#exit
IPS(config-sig-sig)#exit
IPS(config-sig)#exit
Apply Changes:?[yes]:yes
IPS(config)#exit
IPS#
```

## IDS 4.x Sig 11203/0 Modification Example

```
IPS#config t
IDS(config)#service virtual-sensor-configuration virtualSensor
IDS(config-vsc)#tune-micro-engines
IDS(config-vsc-virtualSensor)#string.tcp
IDS(config-vsc-virtualSensor-STR)#signatures SIGID 11203
IDS(config-vsc-virtualSensor-STR-sig)#servicePorts 6666,6667,6668,18067,22522
IDS(config-vsc-virtualSensor-STR-sig)#exit
IDS(config-vsc-virtualSensor-STR)#exit
IDS(config-vsc-virtualSensor)#exit
Apply Changes:[yes]:yes
IDS(config-vsc)#exit
IDS(config)#exit
IDS#
```

**Note:** Although TCP ports 18067 and 22522 have been seen most prevalently for the IRC Bot Command & Control channel new/modified Bots may use different port numbers.

## IDS 4.x Signature

Signature pack S245 adds signature 5799/0 for Cisco Intrusion Detection (IDS) 4.X devices. However, the detection algorithm for this signature differs between the IDS 4.x and IPS 5.x platforms due to enhanced features available in IPS 5.x. The 5799/0 signature is disabled by default in IDS 4.x devices because it is more prone to false positives. Depending on traffic flows, signature 5799/0 may degrade performance on lower end 4.x IDS devices.

```
Signature 5799/0 [In IDS 4.x] Severity: HIGH [Disabled by default]
engine: STRING.TCP
ports 139 and 445
```

## Cisco Security Agent (CSA)

### Mitigation

Cisco Security Agent (CSA) provides mitigation through buffer overflow protection mechanisms that prevent the exploit from doing damage. These mechanisms are a part of the default rule set and are enabled by default. CSA versions 4.0.3.X and later provide prevention capabilities.

The CSA agents must be set in "Protect Mode" (not "Test Mode") mode for successful prevention of this exploit. No updates are required. The specific rules that stop the exploit are:

Buffer overflow protection found in:

**System API control rule** – which is in Rule Module "General Application Permissions – all Security Levels". The description for this rule is: "Network applications, access system functions from a buffer"

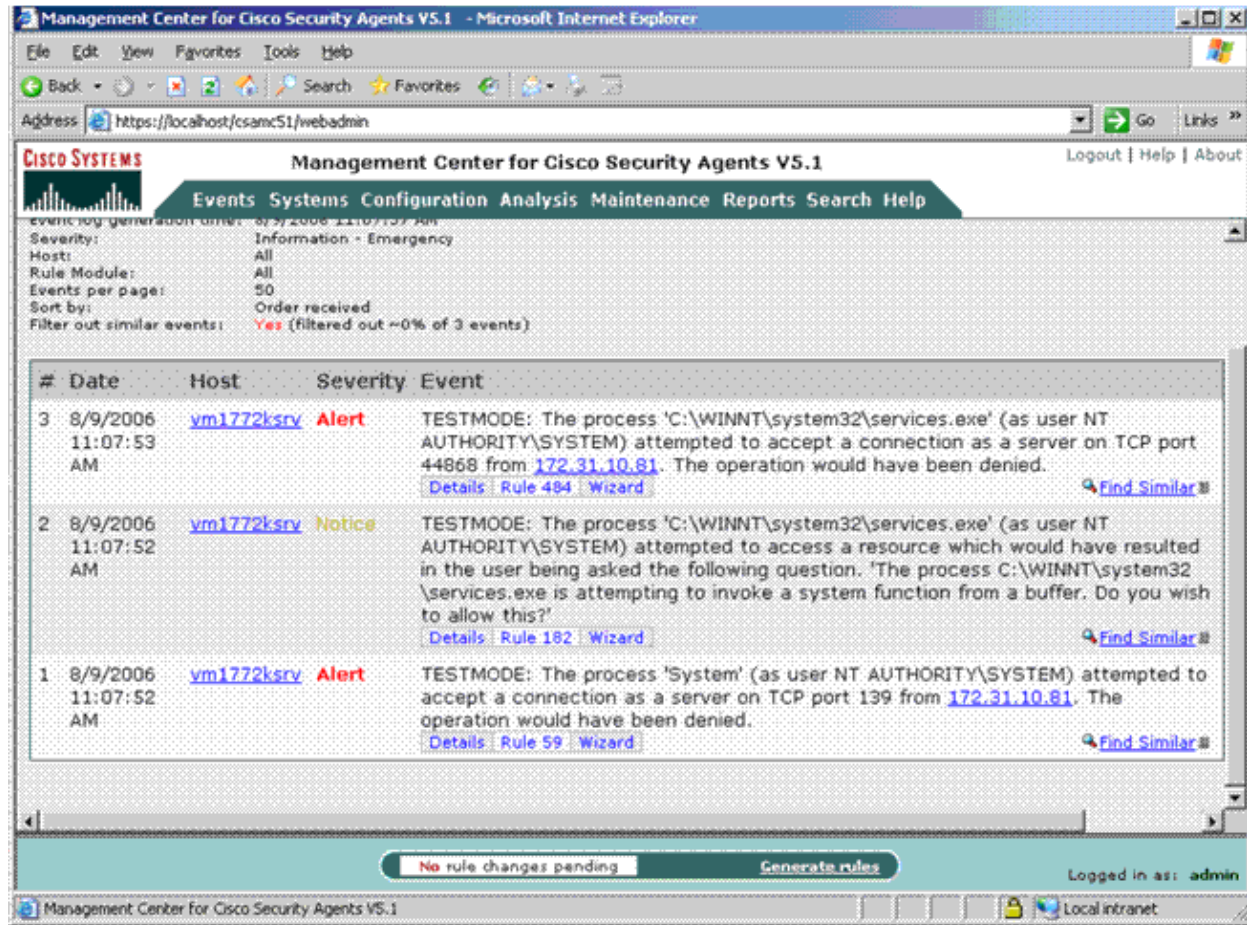
Network access control found in:

**Network access control rule** – which is in Rule Module "System Hardening Module". The description for this rule is: "All applications, server SMB Null Session"

**Network access control rule** – which is in Rule Module "Personal Firewall Module". The description for this rule is: "All applications, server for TCP and UDP services".

## Identification

The following is a screen shot depicting the CSA Management Center (CSAMC) Console providing evidence of the CSA rules that were triggered on the end host.



The screenshot shows the Management Center for Cisco Security Agents V5.1 interface. The main content area displays a list of events for host ym1772ksrv. The events are as follows:

#	Date	Host	Severity	Event
3	8/9/2006 11:07:53 AM	ym1772ksrv	Alert	TESTMODE: The process 'C:\WINNT\system32\services.exe' (as user NT AUTHORITY\SYSTEM) attempted to accept a connection as a server on TCP port 44868 from 172.31.10.81. The operation would have been denied. <a href="#">Details</a> <a href="#">Rule 484</a> <a href="#">Wizard</a> <a href="#">Find Similar</a>
2	8/9/2006 11:07:52 AM	ym1772ksrv	Notice	TESTMODE: The process 'C:\WINNT\system32\services.exe' (as user NT AUTHORITY\SYSTEM) 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?' <a href="#">Details</a> <a href="#">Rule 182</a> <a href="#">Wizard</a> <a href="#">Find Similar</a>
1	8/9/2006 11:07:52 AM	ym1772ksrv	Alert	TESTMODE: The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to accept a connection as a server on TCP port 139 from 172.31.10.81. The operation would have been denied. <a href="#">Details</a> <a href="#">Rule 59</a> <a href="#">Wizard</a> <a href="#">Find Similar</a>

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

## Cisco VPN Termination Points

### Mitigation

Site-to-site VPNs should have access control applied on a need-to-know basis instead of an implicit trust model. Therefore, applying an ACL to block TCP/139 and TCP/445 as part of standard VPN configurations is recommended unless business use dictates otherwise. Below is a sample IOS ACL that could be applied to the decrypted VPN traffic as it exits the VPN termination device or to another screening device that is located at the next hop from the VPN termination device.



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

The access list entries shown below include an example for one of the worm variants now being tracked. New variants using different ports are possible and should be filtered using the information below as examples.

Any added access list entries should be implemented as part of a Transit Access Control List that filters transit and edge traffic at network ingress points.

For more information on tACLs, 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 as 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 are attacking the network.

## Network Ingress Inbound Filtering

```
!-- MS06-040 - Block Initial Scanning On Internet-facing Interfaces
!-- Note: When blocking TCP/139 and TCP/445, 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

!-- Block IRCBot.ST (aka W32.Wargbot, IRC-Mocbot!MS06-040,
!-- W32/Cuebot-L, Backdoor.Win32.IRCBot.st, WORM_IRCBOT.JL) IRC Creation
!-- in the event internal hosts have been compromised as a C&C bot.

access-list 101 deny tcp any any eq 18067

!-- Permit other traffic here,
!-- or include other Transit ACL entries.

access-list 101 permit ip any any
```

## Network Ingress Outbound Filtering

```
!-- MS06-040 - Block Initial Scanning By Infected Hosts

access-list 110 deny tcp any any eq 139
access-list 110 deny tcp any any eq 445

!-- Block outbound IRC Requests to attacking IRCBot.ST
!-- (aka W32.Wargbot, IRC-Mocbot!MS06-040, W32/Cuebot-L, Backdoor.Win32.IRCBot.st,
!-- WORM_IRCBOT.JL) IRC server.

access-list 110 permit tcp <trusted network address block>
    <trusted network block wildcard> any eq 18067 established
access-list 110 deny tcp any any eq 18067

!-- Permit other traffic here,
!-- or include other Transit ACL entries.

access-list 110 permit ip any any

!-- Apply the access-lists to the interface.

interface serial 2/0
ip access-group 101 in
ip access-group 110 out
```

# Interface Access-lists

Any device capable of providing access control is positioned to deter attempted exploitation of this issue.

## Mitigation

With Transit Access-lists, Cisco IOS routers can be configured with interface access-lists to drop packets that could potentially be used to exploit (and contain the spread of) this issue.



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

The access list entries shown below include an example for one of the worm variants now being tracked. New variants using different ports are possible and should be filtered using the information below as examples.

Any added access list entries should be implemented as part of a Transit Access Control List that filters transit and edge traffic at network ingress points.

For more information on tACLs, 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 as 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 are attacking the network.

## Network Ingress Inbound Filtering

```
!-- MS06-040 - Block Initial Scanning On Internet-facing Interfaces  
!-- Note: When blocking TCP/139 and TCP/445, 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  
  
!-- Block IRCBot.ST (aka W32.Wargbot, IRC-Mocbot!MS06-040,  
!-- W32/Cuebot-L, Backdoor.Win32.IRCBot.st, WORM_IRCBOT.JL) IRC Creation  
!-- in the event internal hosts have been compromised as a C&C bot.  
  
access-list 101 deny tcp any any eq 18067  
  
!-- Permit other traffic here,  
!-- or include other Transit ACL entries.  
  
access-list 101 permit ip any any
```

## Network Ingress Outbound Filtering

```
!-- MS06-040 - Block Initial Scanning By Infected Hosts  
  
access-list 110 deny tcp any any eq 139  
access-list 110 deny tcp any any eq 445
```

```

!-- Block outbound IRC Requests to attacking IRCBot.ST
!-- (aka W32.Wargbot, IRC-Mocbot!MS06-040, W32/Cuebot-L,
!--- Backdoor.Win32.IRCBot.st, WORM_IRCBOT.JL) IRC server.

access-list 110 permit tcp <trusted network address block>
    <trusted network block wildcard> any eq 18067 established
access-list 110 deny tcp any any eq 18067

!-- Permit other traffic here,
!-- or include other Transit ACL entries.

access-list 110 permit ip any any

!-- Apply the access-lists to the interface.

interface serial 2/0
ip access-group 101 in
ip access-group 110 out

```

Please note that filtering traffic with an interface access list will elicit the transmission of ICMP unreachable messages back to the source of the filtered traffic. This could have the undesired side effect of high CPU utilization since the device needs to generate 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 1 per 500 ms using the global configuration command **ip icmp rate-limit unreachable <1-4294967295 millisecond>**.

## Identification

With a Transit Access-list, once the interface access-list 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.

Example output for **show access-list 101**:

```

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)
30 deny tcp any any eq 18067
40 permit ip any any

```

In the above example, 100 TCP/139 packets and 141 TCP/445 packets have been dropped by the access-list configured inbound on interface serial 2/0.

## NetFlow

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

```

SC1-Cat6506a#show ip cache flow

```

```

-----
MSFC:
IP packet size distribution (2384 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .000 .962 .036 .001 .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, 4456704 bytes
62 active, 65474 inactive, 2300 added
42112 aged polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds

```

```

IP Sub Flow Cache, 270664 bytes
62 active, 16322 inactive, 2300 added, 2300 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-other	2232	0.0	1	40	0.0	0.0	15.5
ICMP	6	0.0	15	84	0.0	14.7	15.5
Total:	2238	0.0	1	41	0.0	0.0	15.5

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Vl936	192.0.2.6	Vl600	10.89.236.52	06	1E19	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.78	06	1D07	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.94	06	1C2A	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.102	06	1DD4	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.118	06	1DA0	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.134	06	1D4E	01BD	1
Vl936	192.0.2.6	Vl600	10.89.236.150	06	1C0C	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.174	06	1C04	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.190	06	1D76	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.206	06	1A6A	01BD	1
Vl936	192.0.2.6	Vl600	10.89.236.222	06	1A03	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.230	06	1B84	01BD	1

```
----- Output Truncated -----
```

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

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

```

SC1-Cat6506a#show ip cache flow | inc SrcIf|008B|01BD

```

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Vl936	192.0.2.6	Vl600	10.89.236.52	06	1E19	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.78	06	1D07	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.94	06	1C2A	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.102	06	1DD4	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.118	06	1DA0	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.134	06	1D4E	01BD	1
Vl936	192.0.2.6	Vl600	10.89.236.150	06	1C0C	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.174	06	1C04	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.190	06	1D76	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.206	06	1A6A	01BD	1
Vl936	192.0.2.6	Vl600	10.89.236.222	06	1A03	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.230	06	1B84	01BD	1
Vl936	192.0.2.6	Vl600	10.89.236.246	06	1928	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.6	06	19AB	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.22	06	18ED	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.46	06	1997	01BD	1
Vl936	192.0.2.6	Vl600	10.89.236.161	06	1757	008B	1
Vl936	192.0.2.6	Vl600	10.89.236.221	06	17E3	008B	1

## 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	2006–August–21	Updated mitigation information for Cisco ASA and PIX Firewalls, Cisco Intrusion Prevention System, Cisco Security Agent, Cisco VPN Termination Points, Interface Access Lists. Added section for NetFlow.
Revision 1.0	2006–August–14	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

- **IPS 5.x Signature Downloads ( registered customers only)**
- **IDS 4.x Signature Downloads ( registered customers only)**
- **Signatures by Release Version ( registered customers only)**
- **Microsoft Security Bulletin MS06–040: Vulnerability in Server Service Could Allow Remote Code Execution (921883)**
- **Microsoft Security Advisory (922437): Exploit Code Published Affecting the Server Service**
- **Cisco Systems IntelliShield Vulnerability Alert (IntelliShield customers only)**

---

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Aug 21, 2006

Document ID: 70997

---