

# SAFE RPC DCOM/W32/Blaster Attack Mitigation

This document discusses the recently released Microsoft RPC DCOM attack and the W32/Blaster worm and their effects on the network and its hosts. Today, numerous technologies are available for use in Cisco products that mitigate the effects of these attacks. These include not only security technologies such as intrusion detection and packet filtering, but also virtual LAN (VLAN) segmentation and packet classification. In addition to these technologies the SAFE Blueprint from Cisco® combines security best practices and secure network design to mitigate attacks like the RPC DCOM exploit, the W32/Blaster worm, and other network attacks.

This paper contains much of the same information discussed in previous SAFE “in-action” white papers posted at:

[www.cisco.com/go/safe](http://www.cisco.com/go/safe)

This is important to note because the core mitigation techniques stay the same as new exploits are released.

## RPC DCOM Background and Function

A flaw in a section of Microsoft’s RPC code dealing with message exchange over TCP/IP results in the incorrect handling of malformed messages. This flaw is a stack-based buffer overflow occurring in a low-level Distributed Component Object Model (DCOM) interface within the RPC process listening on TCP/IP port 135. This interface is also reachable through ports TCP 139 and 445. This is a core function of the Windows kernel and cannot be disabled.

DCOM is a protocol enabling Microsoft software components to communicate and includes Internet protocols such as HTTP directly over a network. The vulnerability results because the Windows RPC service does not properly check message inputs under certain circumstances. By sending a malformed RPC message, an attacker can cause the RPC service on a device to fail in such a way that arbitrary code could be executed.

Successful exploitation of this vulnerability allows an attacker to run code with Local System privileges (equivalent to a UNIX root). This allows an attacker to install programs, view, change, or delete data, as well as create new accounts with full privileges. Because RPC is active by default on all versions of the Windows operating system, any user who can deliver a malformed TCP request to an RPC interface of a vulnerable computer could attempt to exploit the vulnerability. It is even possible to trigger this vulnerability through other means such as logging into an affected system and exploiting the vulnerable component locally.



On Monday, August 11, 2003, a new worm targeting Microsoft Windows systems was released on the Internet. This worm utilizes the recent Microsoft Windows RPC DCOM exploit discussed in this paper. Unlike the previous Microsoft worm, SQL Slammer, this worm's infection rate is significantly lower because of the lessons learned from the SQL Slammer worm.

#### Cisco Recommendations for Mitigating RPC DCOM and W32/Blaster

The RPC DCOM vulnerability was identified and analyzed by members of the Last Stage of Delirium research group. Their initial announcement of the discovery of this vulnerability is available at:

[http://lsd-pl.net/files/get?WINDOWS/win32\\_dcom](http://lsd-pl.net/files/get?WINDOWS/win32_dcom)

Several groups have released the exploit code for this vulnerability. The typical exploit for this vulnerability uses a reverse-Telnet back to the attacker's host to gain complete access to the target.

The most effective method to prevent the exploitation of this vulnerability from the Internet is the use of ingress and egress filters, or access control lists (ACLs) blocking access to ports 135 and 139 (TCP and UDP) as well as port 445 (TCP and UDP). Network administration best practices provide no need for these ports to be directly Internet-accessible.

*Ingress filtering* is typically performed by ACLs on the perimeter of the network. It is used to block access to hosts and services that should not be publicly available. For instance, it is a security best practice to disallow incoming connection requests to hosts or networking devices unless those hosts or devices are actively participating in providing a publicly accessible service.

Pertaining to RPC DCOM, incoming connections would be blocked from accessing any possibly exploitable user systems or non-publicly available servers. Ideally, any public servers are under tight administrative control. Also, they have the latest patches, and access to ports 135 and 139 (TCP and UDP) or port 445 (TCP and UDP) would require the use of a VPN tunnel. Ingress filtering would, in effect, block any exploitation attempts from the Internet of the RPC DCOM vulnerability targeted at user systems. However, trusted systems already infected by the RPC DCOM worm and connecting to the corporate network through a VPN could still infect other systems.

*Egress filtering* is also typically performed by ACLs on the perimeter of the network. This filtering blocks a local host's access outbound from the network. Devices that don't need outbound Internet access, such as most of the networking devices in the network, should not be allowed to initiate outbound connections.

As this pertains to RPC DCOM, if a device is compromised it will not be able to launch a reverse-Telnet back to the attacker's system because the traffic will be intercepted and dropped at the network perimeter. For more information about access control and filtering, see the SAFE Blueprint white papers.

A sample ingress and egress filter rule to add to existing ACLs is provided in the configuration section at the end of this paper.

After further worm infection has been prevented through the use of ingress and egress filters, the next step is identifying and tracking vulnerable hosts and systems that may already be infected.



The first and most effective manner in which to mitigate the RPC DCOM attack is to patch all systems that are vulnerable. This patching is difficult with uncontrolled user systems in the local network and even more troublesome if they are remotely connected to the network through a VPN or remote access server. However, determining which systems are exploitable can be simplified by the use of security auditing tools that look for vulnerabilities such as the ones listed at the end of this paper.

Scanning for systems that may be running the Microsoft RPC Service helps to quickly identify potentially vulnerable hosts. After these vulnerable systems are identified, they can be patched to remove the vulnerability. Information about attack mitigation on Microsoft products is available at:

<http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp>

#### Additional Microsoft RPC Attacks

The RPC DCOM exploitation is one of two significant attacks currently affecting the Microsoft Windows product suite. The second attack is a denial of service (DoS). This attack uses a similar vector as the RPC DCOM attack by sending a malformed message to the DCOM\_RemoteGetClassObject interface. The result, however, is that the RPC service stops because of the malformed message and requires the system to be rebooted to restore the service.

In both the current RPC DCOM vulnerabilities the exploit code for these attacks is widely available. As always, it is prudent for network engineers as well as management to take the necessary steps to protect their networks to the greatest extent possible. These steps can include some, if not all, of the technologies discussed in this paper. The SAFE Blueprint from Cisco provides enterprises and service providers with a starting point with which to build secure, resilient networks.

If it is not possible to patch all systems in a timely manner when there is a newly discovered vulnerability in a service, consider deploying the technologies discussed in the “Security Technologies” section. Consider using these technologies proactively to mitigate future attacks by variants of the RPC DCOM exploit or other attacks.

#### Security Technologies

This section discusses the technologies available in products from Cisco and other companies to mitigate RPC DCOM and other attacks. To learn more about any of these technologies, or for RPC DCOM mitigating configurations, see the SAFE Blueprint white papers at:

<http://www.cisco.com/go/safe>

#### Host Intrusion Prevention System

The Cisco Systems host intrusion prevention system (HIPS), Cisco Security Agent, operates by detecting attacks that occur on a host on which it is installed. It works by intercepting application resource requests to the operating system to make a real-time allow and deny decisions according to the defined application security policy. The HIPS responds based upon which system it is installed on:

- The default CSA 4.0 server and desktop policies stop successful execution of this attack.
- On servers, the default server policy prevents the SVCHOST from attempting to execute CMD.exe. This prevents the exploit shell code from running.
- On desktop systems the default desktop policy prevents the SVCHOST from accepting a connection on port 4444. Additional protection is provided by the default policy’s prevention of any application from executing CMD.exe.



Because of the sensitive nature of the SVCHOST process in the proper operation of Windows, the Cisco Security Agent detects the overflow but does not terminate the SVCHOST process. Instead, Cisco Security Agent prevents the host from being exploited by terminating the CMD.exe process that the buffer overflow in the SVCHOST process creates because of the exploit.

It may appear that deploying HIPS has the same problem with exploitation mitigation as discussed previously for applying system patches. However, HIPS clients are significantly easier and less obtrusive to install on running systems, and they are less likely to require system interruptions or reboots. To target specific systems for HIPS installation for the current problem, use a network security scanner to identify those systems that are running critical services. To mitigate future network attacks beyond RPC DCOM, consider installing HIPS on critical servers.

### Network-Based Intrusion Detection System

The network-based intrusion detection system (NIDS) operates by first detecting an attack occurring at the network level and then either taking a corrective action or notifying a management system where an administrator can take action. Attacks are discovered by looking for their signatures in traffic flows in the network. Attack detection triggers NIDS to send an alarm and then take a pre-configured action. The two possible actions are shunning and TCP resets. Because NIDS is a passive monitoring mechanism in the data path (meaning it receives a copy of a packet as it traverses through the network versus routing the packet), NIDS cannot filter the first packet in an attack. Subsequent packets can be filtered using a feature known as shunning, which modifies the upstream access-control device to block any further access from the IP address of the attacking system. TCP reset attempts to tear down the TCP connection by sending a fabricated reset that appears to be from the receiving device to the attacking device.

For more information as well as special considerations, refer to the SAFE Blueprint white papers before enabling shunning in a network. For more information about NIDS, see:

<http://www.cisco.com/go/ids>

### Access Control

*Stateful firewalling* provides numerous security features to proactively mitigate the RPC DCOM. First, the stateful inspection engine can control connection attempts at a level more granular than normal by validating proper protocol adherence. If ingress filtering is not used to block external inbound access to vulnerable systems, then outbound filtering should be used to restrict vulnerable hosts from initiating outbound connections. This limits the ability of an attacker to gain command line access to the host, as well as limits the W32/Blaster worm's capability to spread.

### Private VLANs

Private VLANs work by limiting which ports within a VLAN can communicate with other ports in the same VLAN. Typically, private VLANs are deployed so that the hosts on a given segment can communicate only with their default gateway and not the other hosts on the network. For instance, if an attacker compromises a Microsoft server using the RPC DCOM exploit, the attacker would not be able to gain access to other Microsoft servers in the same VLAN, even though they exist in the same network segment. This access control, carried out by assigning hosts to either an isolated port or a community port, is an effective way to mitigate the effects of a single compromised host. Isolated ports can communicate only with promiscuous ports (typically the router). Community ports can communicate with the promiscuous port and other ports in the same community.

For more information about private VLANs, go to:

<http://www.cisco.com/warp/public/473/90.shtml>



## Additional Cisco Networking Technologies to Assist in Mitigating the RPC DCOM Exploit and W32/Blaster

### Network-Based Application Recognition

Network-based application recognition (NBAR) is a classification engine in Cisco IOS® Software that can recognize a wide variety of application-level protocols, including the Microsoft NetBIOS protocol and protocols that use dynamic port assignments. After the traffic has been classified by NBAR, appropriate QoS policies can be applied to the traffic classes. Unlike NIDS, NBAR can immediately classify the NetBIOS traffic and drop the packet before it reaches the server. NBAR can be used inbound to mitigate the effects of the RPC DCOM exploit.

For more information about NBAR, see:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e2/nbar2e.htm>

### NetFlow

NetFlow switching is a high-performance, network-layer switching path that can capture a wide range of traffic statistics including user, protocol, port, and type-of-service information. This information can be used to identify network traffic patterns and help network engineers respond to attacks such as RPC DCOM.

For more information about how to configure NetFlow, see:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products\\_configuration\\_guide\\_chapter09186a00800880f9.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products_configuration_guide_chapter09186a00800880f9.html)

### Committed Access Rate

Analysis of the W32/Blaster worm indicates that it contains code to launch a DoS attack against the Web site *windowsupdate.microsoft.com*. Committed Access Rate (CAR) can be used to reduce the effects of the attack. CAR can rate-limit traffic based on a set of criteria and provides for configurable actions such as transmit, drop, set precedence, or set QoS group when the traffic meets or exceeds the rate limit. These criteria include such metrics as incoming interface, IP Precedence, QoS group, or IP access list criteria, as well as others. CAR performs two QoS functions:

- Bandwidth management through rate-limiting
- Packet classification

By using CAR, network engineers can classify and control traffic into and out of their networks. For more information about CAR, see:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products\\_configuration\\_guide\\_chapter09186a00800c75ce.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800c75ce.html)



## The SAFE Blueprint from Cisco

The SAFE Blueprint from Cisco uses all the security technologies listed above to mitigate the RPC DCOM exploit attack. For this reason, the SAFE Blueprint is “RPC DCOM safe.” Ingress and egress filtering is applied not only at the network edge but also between virtually all SAFE Blueprint modules. This filtering restricts outbound access from infected servers and inbound infection attempts against user systems.

Using firewalls protects both the user and server segments in addition to the filtering and provides distributed DoS connection rate limiting for the public servers. NIDS is deployed not only in all public segments to identify RPC DCOM attack attempts but also behind the network edge filtering. HIPS is installed on all publicly available servers and even critical internal servers that do not have Internet access to guard against possible infection from uncontrolled user systems. Private VLANs are deployed in public-service segments where multiple public servers are available to guard against trust exploitation.

## Conclusion

The technologies discussed in this paper mitigate not only the potential damage the RPC DCOM exploit can cause, but also virtually any attack. It is important to remember that security has its place throughout the infrastructure, and the discussed technologies prove this. Protecting a network and its resources against attacks like the RPC DCOM exploit is only the first step. It is necessary to be proactive about security to protect a network against this worm as well as future network attacks.

Establishing a security policy, implementing some of the discussed features, and regular in-house or outsourced posture assessments will secure a network and keep it secure. This document has addressed a small sampling of the documented security and network design best practices available from Cisco. For additional information about securing your network, see the SAFE Blueprint at:

[www.cisco.com/go/safe](http://www.cisco.com/go/safe)

As with any feature, ensure that all devices have sufficient CPU resources available before enabling any of the features discussed in this paper.

As a special note, the SAFE Blueprint from Cisco was released in October 2000. No design or implementation modifications were required to address the RPC DCOM vulnerability. Only NIDS signature updates at regular intervals were necessary to detect the RPC DCOM exploit. This and other high-profile network exploits constantly provide reminders that designing network security reactively is not recommended. Only by taking a comprehensive approach to network security founded on good security policy decisions can an organization be assured that the risks taken are known, and that virtually any potential threat can be effectively contained.



## Configuration Information

This section provides sample configurations for some of the technologies discussed in this paper that were not tested for attack mitigation capabilities as part of SAFE Blueprint or that later required configuration changes. HIPS is not discussed because the mitigation capability it provides is ready to use and requires no additional configuration beyond placing the system in active mode.

### Cisco IOS Software ACLs

The Cisco IOS Software ACLs for mitigating the RPC DCOM exploits are provided below. You must be careful when you consider whether to use the `log-input` argument to the `access-list` command. It is possible to substantially increase the CPU usage on the router because of the logging on the ACL. If router performance degrades due to the introduction of these ACLs, discontinue the logging on the first ACL.

```
access-list 101 deny udp any any eq 135
access-list 101 deny tcp any any eq 135
access-list 101 deny udp any any eq 137
access-list 101 deny tcp any any eq 137
access-list 101 deny udp any any eq 139
access-list 101 deny tcp any any eq 139
access-list 101 deny udp any any eq 445
access-list 101 deny tcp any any eq 445
access-list 101 deny tcp any any eq 593
access-list 101 permit ip any any
```

To block outbound TFTP traffic to prevent the worm version of the exploit from downloading code to a newly infected host:

```
access-list 102 deny udp any any eq 69
```

To block outbound traffic to port 4444/TCP that the exploit uses to provide command line access to a Windows target host:

```
access-list 102 deny tcp any any eq 4444
```

A more fine-tuned approach would be to create an ACL for the offending RPC DCOM traffic, and then use a class-based policing to drop the packets at the ingress interface.

1. Create an ACL.

```
access-list 101 deny udp any any eq 135
access-list 101 deny tcp any any eq 135
access-list 101 deny udp any any eq 137
access-list 101 deny tcp any any eq 137
access-list 101 deny udp any any eq 139
access-list 101 deny tcp any any eq 139
access-list 101 deny udp any any eq 445
access-list 101 deny tcp any any eq 445
access-list 101 deny tcp any any eq 593
access-list 101 permit ip any any
```



2. Match on ACL and packet length.

```
class-map match-all rpc_dcom
match access-group 101
```

3. Use class-based policing to drop matching packets at the ingress interface.

```
policy-map drop-rpc-dcom
class rpc_dcom
police 8000 1000 1000 conform-action drop exceed-action drop violate-action drop
```

### NIDS Attack Signatures

The Cisco IDS Network Security Database (NSDB) includes a signature for the Microsoft Windows RPC DCOM exploit (sig 3327). It is available in IDS signature update S49.

The following custom signature string can be added to address this worm:

```
Engine      : STRING.UDP
SigName     : MS Blast Worm TFTP Request
ServicePorts : 69
RegexString : \x00\x01[Mm][Ss][Bb][Ll][Aa][Ss][Tt][.][Ee][Xx][Ee]\x00
Direction  : ToService
```

For registered customers, the following service pack includes this signature for the RPC DCOM exploit. To reduce the number of false positives on this signature, consider restricting this signature's inspection of ports to 137, 139, and 445 only.

<ftp://ftp-sj.cisco.com/cisco/crypto/3DES/ciscosecure/ids/4.x/IDS-sig-4.1-1-S49.rpm.pkg>

### NBAR

NBAR provides for the creation of a custom protocol to monitor traffic not normally associated with NBAR. The following configuration is an example.

#### Custom Protocol in NBAR

1. Create a custom protocol.

```
ip nbar port-map netbios tcp 135 139 445
ip nbar port-map netbios udp 135 139 445
```

2. Create a class-map.

```
class-map match-all rpc_dcom
match protocol netbios
```



3. Use class-based policing to drop the matching packets at the ingress interface.

```
policy-map drop-rpc-dcom
class rpc_dcom
police 8000 1000 1000 conform-action drop exceed-action drop violate-action drop
```

## NetFlow

NetFlow can be configured and enabled on a variety of Cisco routers. The following configuration provides a general description of how to configure NetFlow. Consult the Cisco Web site ([www.cisco.com](http://www.cisco.com)) for more specific information about a particular router platform. To configure NetFlow on a NetFlow-capable router:

```
Router# config t
Router# (config) interface serial 0/1
Router#(config-if) ip route-cache flow
Router#(config-if) exit
Router#(config) exit
Router#
```

After NetFlow has been enabled on the router, the information can be exported to a variety of network management applications. To export NetFlow statistics:

```
Router# (config) ip flow-export 192.168.155.1 700
```

To view NetFlow statistics for port 135, 139, and 445:

```
Router# show ip cache flow | include 0087
Router# show ip cache flow | include 0089
Router# show ip cache flow | include 01BD
```

## CAR

Like NetFlow, CAR can be configured on a variety of Cisco routers. The following configuration is an example:

```
Router# (config) access-list 150 permit udp any any eq 135
Router# (config) access-list 150 permit udp any any eq 139
Router# (config) access-list 150 permit tcp any any eq 135
Router# (config) access-list 150 permit tcp any any eq 135
Router# (config) access-list 150 permit udp any any eq 445
Router# (config) access-list 150 permit tcp any any eq 445
Router# (config) access-list 150 deny ip any any
Router# (config) interface fastEthernet 0/0
Router# (config-if) rate-limit input access-group rate-limit 150 8000 1500 20000 conform-action
drop exceed-action drop
Router# (config-if) exit
Router# (config) exit
Router#
```

## Links to Additional Information

Cisco PSIRT advisories for Microsoft RPC DCOM vulnerability and worm:

- <http://www.cisco.com/warp/public/707/cisco-sn-20030814-blaster.shtml>
- [http://www.cisco.com/en/US/partner/products/sw/netmgts/ps533/products\\_field\\_notice09186a00801ab664.shtml](http://www.cisco.com/en/US/partner/products/sw/netmgts/ps533/products_field_notice09186a00801ab664.shtml)
- [http://www.cisco.com/en/US/partner/products/sw/netmgts/ps533/prod\\_release\\_note09186a00801aca24.html](http://www.cisco.com/en/US/partner/products/sw/netmgts/ps533/prod_release_note09186a00801aca24.html)

NIDS signature ID for the RPC DCOM exploit:

- <http://www.cisco.com/go/csec>
  - Search for ID 3327.

HIPS:

- <http://www.cisco.com/en/US/partner/products/sw/secursw/ps5057/index.html>

Microsoft response to the RPC DCOM vulnerability and required patches:

- <http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp>
- <http://support.microsoft.com/?kbid=823980>

Last Stage of Delirium announcement of the Microsoft RPC DCOM vulnerability:

- [http://lsd-pl.net/files/get?WINDOWS/win32\\_dcom](http://lsd-pl.net/files/get?WINDOWS/win32_dcom)

Computer Emergency Response Team (CERT) information about the Microsoft RPC DCOM vulnerability:

- <http://www.cert.org/advisories/CA-2003-19.html>

## Links to Cisco Products and Services

NIDS:

- <http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz>

Information about Cisco security products and security consulting:

- <http://www.cisco.com/go/security>
- <http://www.cisco.com/go/securityconsulting>

The Cisco PIX<sup>®</sup> firewall:

- <http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/>



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

European Headquarters  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

**Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland  
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland  
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.  
(0304R) N2/VT/LW4986 08/03