

# [NT] Vulnerability in Server Service Allows Code Execution (MS08-067)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-10/msg00069.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 24 Oct 2008 00:20:25 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Vulnerability in Server Service Allows Code Execution (MS08-067)

---

## SUMMARY

This security update resolves a privately reported vulnerability in the Server service. The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit. Firewall best practices and standard default firewall configurations can help protect network resources from attacks that originate outside the enterprise perimeter.

This security update is rated Critical for all supported editions of Microsoft Windows 2000, Windows XP, Windows Server 2003, and rated Important for all supported editions of Windows Vista and Windows Server 2008. For more information, see the subsection, Affected and Non-Affected Software, in this section.

## DETAILS

Affected Software:

## [NT] Vulnerability in Server Service Allows Code Execution (MS08-067)

- \* Microsoft Windows 2000 Service Pack 4 – Remote Code Execution – Critical – MS06-040
- \* Windows XP Service Pack 2 – Remote Code Execution – Critical – MS06-040
- \* Windows XP Service Pack 3 – Remote Code Execution – Critical – None
- \* Windows XP Professional x64 Edition – Remote Code Execution – Critical – MS06-040
- \* Windows XP Professional x64 Edition Service Pack 2 – Remote Code Execution – Critical – None
- \* Windows Server 2003 Service Pack 1 – Remote Code Execution – Critical – MS06-040
- \* Windows Server 2003 Service Pack 2 – Remote Code Execution – Critical – None
- \* Windows Server 2003 x64 Edition – Remote Code Execution – Critical – MS06-040
- \* Windows Server 2003 x64 Edition Service Pack 2 – Remote Code Execution – Critical – None
- \* Windows Server 2003 with SP1 for Itanium-based Systems – Remote Code Execution – Critical – MS06-040
- \* Windows Server 2003 with SP2 for Itanium-based Systems – Remote Code Execution – Critical – None
- \* Windows Vista and Windows Vista Service Pack 1 – Remote Code Execution – Important – None
- \* Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1 – Remote Code Execution – Important – None
- \* Windows Server 2008 for 32-bit Systems\* – Remote Code Execution – Important – None
- \* Windows Server 2008 for x64-based Systems\* – Remote Code Execution – Important – None
- \* Windows Server 2008 for Itanium-based Systems – Remote Code Execution – Important – None

\*Windows Server 2008 server core installation affected. For supported editions of Windows Server 2008, this update applies, with the same severity rating, whether or not Windows Server 2008 was installed using the Server Core installation option. For more information on this installation option, see Server Core. Note that the Server Core installation option does not apply to certain editions of Windows Server 2008; see Compare Server Core Installation Options.

### Server Service Vulnerability – CVE-2008-4250

A remote code execution vulnerability exists in the Server service on Windows systems. The vulnerability is due to the service not properly handling specially crafted RPC requests. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

#### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250>>  
CVE-2008-4250

## [NT] Vulnerability in Server Service Allows Code Execution (MS08-067)

### Mitigating Factors for Server Service Vulnerability – CVE-2008-4250

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- \* Firewall best practices and standard default firewall configurations can help protect network resources from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

- \* On Windows Vista and Windows Server 2008, the vulnerable code path is only accessible to authenticated users. This vulnerability is not liable to be triggered if the attacker is not authenticated.

### Workarounds for Server Service Vulnerability – CVE-2008-4250

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

- \* Disable the Server and Computer Browser services

Disabling the Computer Browser and Server service on the affected systems will help protect systems from remote attempts to exploit this vulnerability.

You can disable these services by using the following steps:

1. Click Start, and then click Control Panel (or point to Settings and then click Control Panel).
2. Double-click Administrative Tools.
3. Double-click Services.
4. Double-click Computer Browser Service.
5. In the Startup type list, click Disabled.
6. Click Stop, and then click OK.
7. Repeat steps 4-6 for the Server service

**Impact of Workaround.** If the Computer Browser service is disabled, any services that explicitly depend on the Computer Browser service may log an error message in the system event log. For more information about the Computer Browser service, see Microsoft Knowledge Base Article 188001. If the Server service is disabled, you will not be able to share files or printers from your computer. However, you will still be able to view and

## [NT] Vulnerability in Server Service Allows Code Execution (MS08-067)

use file shares and printer resources on other systems.

How to undo the workaround. You can enable these services by using the following steps:

1. Click Start, and then click Control Panel (or point to Settings, and then click Control Panel).
2. Double-click Administrative Tools.
3. Double-click Services.
4. Double-click Computer Browser Service.
5. In the Startup type list, click Automatic.
6. Click Start, and then click OK.
7. Repeat steps 4-6 for the Server service

\* On Windows Vista and Windows Server 2008, filter the affected RPC identifier

In addition to blocking ports with the Windows Firewall, the Windows Vista and Windows Server 2008 editions can selectively filter RPC Universally Unique Identifiers (UUID). To prevent this vulnerability, add a rule that blocks all RPC requests with the UUID equal to 4b324fc8-1670-01d3-1278-5a47bf6ee188. This is accomplished through the network shell. To access the network shell, run the following command from an elevated command prompt:

```
netsh
```

Once in the netsh environment, enter the following commands:

```
netsh>rpc
netsh rpc>filter
netsh rpc filter>add rule layer=um actiontype=block
netsh rpc filter>add condition field=if_uuid matchtype=equal
data=4b324fc8-1670-01d3-1278-5a47bf6ee188
netsh rpc filter>add filter
netsh rpc filter>quit
```

The Filter Key is a randomly generated UUID specific to each system. To confirm the filter is in place, run the following command from an elevated command prompt:

```
netsh rpc filter show filter
```

If the commands are successful, the system displays the following information:

## [NT] Vulnerability in Server Service Allows Code Execution (MS08-067)

Listing all RPC Filters.

```
-----  
filterKey: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx  
displayData.name: RPCFilter  
displayData.description: RPC Filter  
filterId: 0x12f79  
layerKey: um  
weight: Type: FWP_EMPTY Value: Empty  
action.type: block  
numFilterConditions: 1
```

Where filterKey: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx equates to the randomly generated UUID relevant to your system.

Impact of workaround. Certain applications that rely on the Microsoft Server Message Block (SMB) Protocol may not function as intended. However, you will still be able to view and use file shares and printer resources on other systems.

How to undo the workaround. Run the following command from an elevated command prompt:

```
netsh rpc filter delete filter xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

Where filterKey: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx equates to the randomly generated UUID relevant to your system.

\* Block TCP ports 139 and 445 at the firewall

These ports are used to initiate a connection with the affected component. Blocking TCP ports 139 and 445 at the firewall will help protect systems that are behind that firewall from attempts to exploit this vulnerability. Microsoft recommends that you block all unsolicited inbound communication from the Internet to help prevent attacks that may use other ports. For more information about ports, see TCP and UDP Port Assignments.

Impact of workaround. Several Windows services use the affected ports. Blocking 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 use SMB (CIFS)
- \* Applications that use 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

## [NT] Vulnerability in Server Service Allows Code Execution (MS08-067)

- \* Indexing Service
- \* Performance Logs and Alerts
- \* Systems Management Server
- \* License Logging Service

\* To help protect from network-based attempts to exploit this vulnerability, use a personal firewall, such as the Internet Connection Firewall

All supported editions of Windows Vista come with Windows Firewall, a two-way firewall that is automatically enabled.

For all supported editions of Windows XP and Windows Server 2003, use the Internet Connection Firewall feature to help protect your Internet connection by blocking unsolicited incoming traffic. Microsoft recommends that you block all unsolicited incoming communication from the Internet. In Windows XP Service Pack 2 and Windows XP Service Pack 3, this feature is called the Windows Firewall.

By default, the Windows Firewall feature in Windows XP helps protect your Internet connection by blocking unsolicited incoming traffic. We recommend that you block all unsolicited incoming communication from the Internet.

To enable the Windows Firewall feature by using the Network Setup Wizard, follow these steps:

1. Click Start, and then click Control Panel.
2. Double-click Network Connections and then click Change Windows Firewall Settings.
3. On the General tab, ensure that the On (recommended) value is selected. This will enable the Windows Firewall.
4. Once the Windows Firewall is enabled, select Don't allow exceptions to prohibit all incoming traffic.

For Windows Server 2003 systems, configure Internet Connection Firewall manually for a connection using the following steps:

1. Click Start, and then click Control Panel.
2. In the default Category View, click Networking and Internet Connections, and then click Network Connections.
3. Right-click the connection on which you want to enable Internet Connection Firewall, and then click Properties.
4. Click the Advanced tab.
5. Click to select the Protect my computer or network by limiting or

[NT] Vulnerability in Server Service Allows Code Execution (MS08-067)

preventing access to this computer from the Internet check box, and then click OK.

Note If you want to enable certain programs and services to communicate through the firewall, click Settings on the Advanced tab, and then select the programs, the protocols, and the services that are required.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security.

The original article can be found at:

<http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>

<http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.