

[NT] Vulnerability in RPC Allows Denial of Service (MS07-058)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-10/msg00015.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 10 Oct 2007 19:08:49 +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 RPC Allows Denial of Service (MS07-058)

SUMMARY

A denial of service vulnerability exists in the remote procedure call (RPC) facility due to a failure in communicating with the NTLM security provider when performing authentication of RPC requests.

The vulnerability is documented in its own subsection in the Vulnerability Details section of this bulletin.

DETAILS

Affected Software:

- * Microsoft Windows 2000 Service Pack 4
- * Windows XP Service Pack 2
- * Windows XP Professional x64 Edition
- * Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2
- * Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2
- * Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems

[NT] Vulnerability in RPC Allows Denial of Service (MS07-058)

- * Windows Vista
- * Windows Vista x64 Edition

RPC Authentication Vulnerability Could Allow Denial of Service – CVE-2007-2228:

A denial of service vulnerability exists in the remote procedure call (RPC) facility due to a failure in communicating with the NTLM security provider when performing authentication of RPC requests. An anonymous attacker could exploit the vulnerability by sending a specially crafted RPC authentication request to a computer over the network. An attacker who successfully exploited this vulnerability could cause the computer to stop responding and automatically restart.

Mitigating Factors for RPC Authentication Vulnerability Could Allow Denial of Service – CVE-2007-2228:

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 networks 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.

Workarounds for RPC Authentication Vulnerability Could Allow Denial of Service – CVE-2007-2228:

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:

- * Block the following at the firewall:
 - * UDP ports 135, 137, 138, and 445, and TCP ports 135, 139, 445, and 593
 - * All unsolicited inbound traffic on ports greater than 1024
 - * Any other specifically configured RPC port

These ports are used to initiate a connection with RPC. Blocking them at the firewall will help protect systems that are behind that firewall from attempts to exploit this vulnerability. Also, make sure that you block any other specifically configured RPC port on the remote system. We recommend that you block all unsolicited inbound communication from the Internet to help prevent attacks that may use other ports. For more information about ports that RPC uses, visit the following Web site.

Impact of Workaround: Several Windows services use the affected ports. Blocking connectivity to the ports may cause various applications or

[NT] Vulnerability in RPC Allows Denial of Service (MS07-058)

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

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 Windows Firewall, which is included with Windows XP and with Windows Server 2003.

By default, the Windows Firewall feature in Windows XP and Windows Server 2003 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.

Note If you want to enable certain programs and services to communicate through the firewall, de-select Don't allow exceptions and click the Exceptions tab. On the Exceptions tab, select the programs, protocols, and services that you want to enable.

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)

[NT] Vulnerability in RPC Allows Denial of Service (MS07-058)

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

* To help protect from network-based attempts to exploit this vulnerability, enable advanced TCP/IP filtering on systems that support this feature.

You can enable advanced TCP/IP filtering to block all unsolicited inbound traffic. For more information about how to configure TCP/IP filtering, see <<http://support.microsoft.com/kb/309798>> Microsoft Knowledge Base Article 309798.

* To help protect from network-based attempts to exploit this vulnerability, block the affected ports by using IPsec on the affected systems.

Use Internet Protocol security (IPsec) to help protect network communications. Detailed information about IPsec and about how to apply filters is available in <<http://support.microsoft.com/kb/313190>> Microsoft Knowledge Base Article 313190 and <<http://support.microsoft.com/kb/813878>> Microsoft Knowledge Base Article 813878.

FAQ for RPC Authentication Vulnerability Could Allow Denial of Service – CVE-2007-2228:

What is Microsoft RPC Authentication?

To complete any remote procedure call, all distributed applications must create a binding between the client and the server. Microsoft RPC provides multiple levels of authentication. Depending on the authentication level, the origin of the traffic (which security principal sent the traffic) can be verified when the connection is established, when the client starts a new remote procedure call, or during each packet exchange between the client and server. For additional information on RPC and RPC Authentication please see the following <<http://msdn2.microsoft.com/en-us/library/aa378646.aspx>> MSDN Article.

What is the scope of the vulnerability?

This is a denial of service vulnerability. An attacker who exploited this vulnerability could cause the affected system to stop responding and automatically restart. Note that the denial of service vulnerability would not allow an attacker to execute code or to elevate their user rights, but

[NT] Vulnerability in RPC Allows Denial of Service (MS07-058)

it could cause the affected system to stop accepting requests.

What causes the vulnerability?

Specially crafted packets using the NTLMSSP authentication type can cause the RPC service to fail in such a way that could cause the system to restart.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause a user's system to become non-responsive and restart.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted RPC message and sending the message to an affected system over an affected TCP/UDP port. The message could then cause the RPCSS service to stop responding and cause the vulnerable system to fail in such a way that it could cause a denial of service.

Could the vulnerability be exploited over the Internet?

Yes. An attacker could try to exploit this vulnerability over the Internet. Firewall best practices and standard default firewall configurations can help protect against attacks that originate from the Internet. Microsoft has provided information about how you can help protect your system. End users can visit <http://go.microsoft.com/fwlink/?LinkId=85102> Security At Home. IT professionals can visit <http://go.microsoft.com/fwlink/?LinkId=21171> TechNet Security Center.

What systems are primarily at risk from the vulnerability?

Both workstations and servers are at risk. Systems that allow RPC traffic from untrusted networks could be at more risk.

What does the update do?

The update removes the vulnerability by validating the RPC request.

When this security bulletin was issued, had this vulnerability been publicly disclosed?

No. Microsoft received information about this vulnerability through responsible disclosure.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Security Bulletin MS07-058.

[NT] Vulnerability in RPC Allows Denial of Service (MS07-058)

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/ms07-058.msp>>

<http://www.microsoft.com/technet/security/bulletin/ms07-058.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.