

[NT] Buffer Overrun in RPC Interface Could Allow Code Execution

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0064.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/17/03

To: list@securiteam.com

Date: 17 Jul 2003 11:48:05 +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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Buffer Overrun in RPC Interface Could Allow Code Execution

SUMMARY

Remote Procedure Call (RPC) is a protocol used by the Windows operating system. RPC provides an inter-process communication mechanism that allows a program running on one computer to seamlessly execute code on a remote system. The protocol itself is derived from the Open Software Foundation (OSF) RPC protocol, but with the addition of some Microsoft specific extensions.

There is a vulnerability in the part of RPC that deals with message exchange over TCP/IP. The failure results because of incorrect handling of malformed messages. This particular vulnerability affects a Distributed Component Object Model (DCOM) interface with RPC, which listens on TCP/IP port 135. This interface handles DCOM object activation requests that are sent by client machines (such as Universal Naming Convention (UNC) paths) to the server. An attacker who successfully exploited this vulnerability would be able to run code with Local System privileges on an affected system. The attacker would be able to take any action on the system,

Securiteam: [NT] Buffer Overrun in RPC Interface Could Allow Code Execution

including installing programs, viewing changing or deleting data, or creating new accounts with full privileges.

To exploit this vulnerability, an attacker would need to send a specially formed request to the remote computer on port 135.

DETAILS

Affected Software:

- * Microsoft Windows NT 4.0
- * Microsoft Windows NT 4.0 Terminal Services Edition
- * Microsoft Windows 2000
- * Microsoft Windows XP
- * Microsoft Windows Server 2003

Not Affected Software:

- * Microsoft Windows Millennium Edition

Mitigating factors:

* To exploit this vulnerability, the attacker would require the ability to send a specially crafted request to port 135 on the remote machine. For intranet environments, this port would normally be accessible, but for Internet connected machines, port 135 would normally be blocked by a firewall. In the case where this port is not blocked, or in an intranet configuration, the attacker would not require any additional privileges.

* Best practices recommend blocking all TCP/IP ports that are not actually being used. For this reason, most machines attached to the Internet should have port 135 blocked. RPC over TCP is not intended to be used in hostile environments such as the Internet. More robust protocols such as RPC over HTTP are provided for hostile environments.

To learn more about securing RPC for client and server please refer to

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/rpc/rpc/writing_a_secure_rpc_client_or_server.asp
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/rpc/rpc/writing_a_secure_rpc_client_or_server.asp

To learn more about the ports used by RPC, please refer to:

<http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/tcpip/part4/tcpappc.asp>
<http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/tcpip/part4/tcpappc.asp>

Patch availability:

Download locations for this patch

- * Windows NT 4.0 Server –

<http://microsoft.com/downloads/details.aspx?FamilyId=2CC66F4E-217E-4FA7-BDBF-DF77A0B9303F&displaylang=en>
<http://microsoft.com/downloads/details.aspx?FamilyId=2CC66F4E-217E-4FA7-BDBF-DF77A0B9303F&displaylang=en>

- * Windows NT 4.0 Terminal Server Edition –

<http://microsoft.com/downloads/details.aspx?FamilyId=6C0F0160-64FA-424C-A3C1-C9FAD2DC65CA&displaylang=en>
<http://microsoft.com/downloads/details.aspx?FamilyId=6C0F0160-64FA-424C-A3C1-C9FAD2DC65CA&displaylang=en>

- * Windows 2000 –

<http://microsoft.com/downloads/details.aspx?FamilyId=C8B8A846-F541-4C15-8C9F-220354449117&displaylang=en>
<http://microsoft.com/downloads/details.aspx?FamilyId=C8B8A846-F541-4C15-8C9F-220354449117&displaylang=en>

Securiteam: [NT] Buffer Overrun in RPC Interface Could Allow Code Execution

* Windows XP 32 bit Edition –

<<http://microsoft.com/downloads/details.aspx?FamilyId=2354406C-C5B6-44AC-9532-3DE40F69C074&displaylang=en>
<http://microsoft.com/downloads/details.aspx?FamilyId=2354406C-C5B6-44AC-9532-3DE40F69C074&displaylang=en>

* Windows XP 64 bit Edition –

<<http://microsoft.com/downloads/details.aspx?FamilyId=1B00F5DF-4A85-488F-80E3-C347ADCC4DF1&displaylang=en>
<http://microsoft.com/downloads/details.aspx?FamilyId=1B00F5DF-4A85-488F-80E3-C347ADCC4DF1&displaylang=en>

* Windows Server 2003 32 bit Edition –

<<http://microsoft.com/downloads/details.aspx?FamilyId=F8E0FF3A-9F4C-4061-9009-3A212458E92E&displaylang=en>
<http://microsoft.com/downloads/details.aspx?FamilyId=F8E0FF3A-9F4C-4061-9009-3A212458E92E&displaylang=en>

* Windows Server 2003 64 bit Edition –

<<http://microsoft.com/downloads/details.aspx?FamilyId=2B566973-C3F0-4EC1-995F-017E35692BC7&displaylang=en>
<http://microsoft.com/downloads/details.aspx?FamilyId=2B566973-C3F0-4EC1-995F-017E35692BC7&displaylang=en>

What's the scope of the vulnerability?

This is a buffer-overrun vulnerability. An attacker who successfully exploited this vulnerability could gain complete control over a remote computer. This would give the attacker the ability to take any action on the server that they want. For example, an attacker could change Web pages, reformat the hard disk, or add new users to the local administrators group.

To carry out such an attack, an attacker would require the ability to send a malformed message to the RPC service and thereby cause the target machine to fail in such a way that arbitrary code could be executed.

The best defense against remote RPC attacks from the Internet is to configure the firewall to block port 135. RPC over TCP is not intended to be used across hostile environments such as the Internet.

What causes the vulnerability?

The vulnerability results because the Windows RPC service does not properly check message inputs under certain circumstances. This particular failure affects an underlying Distributed Component Object Model (DCOM) interface, which listens on TCP/IP port 135. By sending a malformed RPC message, an attacker could cause the RPC service on a machine to fail in such a way that arbitrary code could be executed. Interface with RPC on the remote machine to fail in such a way that arbitrary code could be executed.

What is DCOM?

The Distributed Component Object Model (DCOM) is a protocol that enables software components to communicate directly over a network. Previously called "Network OLE", DCOM is designed for use across multiple network transports, including Internet protocols such as HTTP. More information about DCOM can be found at the following website:

<<http://www.microsoft.com/com/tech/dcom.asp>>
<http://www.microsoft.com/com/tech/dcom.asp>

What is RPC (Remote Procedure Call)?

Remote Procedure Call (RPC) is a protocol that a program can use to request a service from a program located on another computer in a network.

Securiteam: [NT] Buffer Overrun in RPC Interface Could Allow Code Execution

RPC helps with interoperability because the program using RPC does not have to understand the network protocols that are supporting communication. In RPC, the requesting program is the client and the service-providing program is the server.

What's wrong with Microsoft's implementation of Remote Procedure Call (RPC)?

There is a flaw in a part of RPC that deals with message exchange over TCP/IP. A failure results because of incorrect handling of malformed messages. This particular failure affects an underlying DCOM interface, which listens on TCP/IP port 135. By sending a malformed RPC message, an attacker could cause the RPC service on a machine to fail in such a way that arbitrary code could be executed.

Is this a flaw in the RPC Endpoint Mapper?

No – Although the RPC endpoint mapper listens on TCP port 135, the flaw actually occurs in a low level DCOM interface within the RPC process. The RPC endpoint mapper allows RPC clients to determine the port number currently assigned to a particular RPC service. An endpoint is a protocol port or named pipe on which the server application listens to for client remote procedure calls. Client/server applications can use either well-known or dynamic ports.

Security Bulletin MS03-010 also involved RPC yet you could not fix that vulnerability on Windows NT 4.0. How were you able to fix this vulnerability on Windows NT 4.0?

The flaw in this case lies in an underlying DCOM interface to RPC, and not the overall RPC implementation or the RPC Endpoint Mapper itself. As a result, it was possible to address this vulnerability in Windows NT 4.0 without needing to rearchitect significant portions of the Windows NT 4.0 operating system, as would have been required by a Windows NT 4.0 patch for security bulletin MS03-010.

What could this vulnerability enable an attacker to do?

An attacker who successfully exploited this vulnerability would be able to run code with Local System privileges on an affected system. The attacker would be able to take any action on the system, including installing programs, viewing changing or deleting data, or creating new accounts with full privileges.

How could an attacker exploit this vulnerability?

An attacker could seek to exploit this vulnerability by programming a machine that could communicate with a vulnerable server over TCP port 135 to send a specific kind of malformed RPC message. Receipt of such a message could cause the RPC service on the vulnerable machine to fail in such a way that it could execute arbitrary code.

Who could exploit the vulnerability?

Any user who could deliver a TCP request to port 135 to an affected computer could attempt to exploit the vulnerability. Because RPC requests are on by default in all versions of Windows, this in essence means that

Securiteam: [NT] Buffer Overrun in RPC Interface Could Allow Code Execution

any user who could establish a connection with an affected computer could attempt to exploit the vulnerability.

It could also be possible to access the affected component through another vector, such as one that would involve logging onto the system interactively or by using another application similar that passed parameters to the vulnerable component either locally or remotely.

What does the patch do?

The patch corrects the vulnerability by altering the DCOM interface to properly check the information passed to it.

Workarounds:

Are there any workarounds that can be used to block exploitation of this vulnerability while I am testing or evaluating the patch?

Yes. Although Microsoft urges all customers to apply the patch at the earliest possible opportunity, there are a number of workarounds that can be applied to help prevent the vector used to exploit this vulnerability in the interim.

It should be noted that these workarounds should be considered temporary measures as they just help block paths of attack rather than correcting the underlying vulnerability.

The following sections are intended to provide you with information to help protect your computer from attack. Each section describes the workarounds that you may want to use depending on your computer's configuration.

Each section describes the workarounds available depending on your required level of functionality.

* Block Port 135 at your firewall.

Port 135 is used to initiate an RPC connection with a remote computer. Blocking Port 135 at the firewall will help prevent systems behind that firewall from being attacked by attempts to exploit this vulnerability.

* Internet Connection Firewall

If you are using the Internet Connection Firewall in Windows XP or Windows Server 2003 to protect your Internet connection, it will by default block inbound RPC traffic from the Internet.

* Disable DCOM on all affected machines

When a computer is part of a network, the DCOM wire protocol enables COM objects on that computer to communicate with COM objects on other computers. You can disable DCOM for a particular computer to help protect against this vulnerability, but doing so will disable all communication between objects on that computer and objects on other computers.

If you disable DCOM on a remote computer, you will not be able to remotely access that computer afterwards to reenable DCOM. To reenable DCOM, you will need physical access to that computer.

Securiteam: [NT] Buffer Overrun in RPC Interface Could Allow Code Execution

To manually enable (or disable) DCOM for a computer:

1. Run Dcomcnfg.exe.

If you are running Windows XP or Windows Server 2003 perform these additional steps:

- * Click on the Component Services node under Console Root.
 - * Open the Computers sub-folder.
 - * For the local computer, right click on My Computer and choose Properties.
 - * For a remote computer, right click on the Computers folder and choose New then Computer. * Enter the computer name. Right click on that computer name and choose Properties.
2. Choose the Default Properties tab.
3. Select (or clear) the Enable Distributed COM on this Computer check box.
4. If you will be setting more properties for the machine, click the Apply button to enable (or disable) DCOM. Otherwise, click OK to apply the changes and exit Dcomcnfg.exe.

ADDITIONAL INFORMATION

The information has been provided by

<mailto:0_50144_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C_US@Newsletters.Microsoft.com>
Microsoft Product Security.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

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.