

## Re: deactivating DCOM

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2003-07/1513.html>

---

**From:** Susan Bradley, CPA aka Ebitz SBS Rocks [MVP] ([sbradcpa\\_at\\_pacbell.net](mailto:sbradcpa_at_pacbell.net))

**Date:** 07/21/03

Date: Sun, 20 Jul 2003 22:10:46 -0700

Q1 How do I enable or disable DCOM?

A. The HKEY\_LOCAL\_MACHINE\Software\Microsoft\OLE registry key has "EnabledDCOM" as a named value. By default this value is set to "Y." To disable DCOM, change this value to "N." You can do this in the OLE/COM Object Viewer with the File.System Configuration dialog box. Changing this value requires you to restart your computer.

If EnabledDCOM is not set to "Y," then all cross-computer calls are rejected (the caller, typically, receives an RPC\_S\_SERVER\_UNAVAILABLE return code).

On Windows 95, with DCOM support, there is an additional registry setting that enables or disables incoming remote connections. The registry key is HKEY\_LOCAL\_MACHINE\Software\Microsoft\OLE, and the named value is "EnableRemoteConnections." By default remote connections are disabled (the value is "N"). To enable remote connections to a Windows 95 computer, change this value to "Y." You can do this in the OLE/COM Object Viewer (OLEView) with the File.System Configuration dialog box. Changing this value requires a restart.

You'll have to reboot anyway.... just in case they use another unknown threat vector to get in, I'd rather patch. The exploit is not public at this time....

Bijan Kianifard wrote:

> *Hello to all,*  
>  
> *I recieve this message from eeye digital security and I*  
> *think it is interesting to you:*  
>  
> *Microsoft Remote Procedure Call (RPC) Vulnerability*  
>  
> *Systems Affected*  
> *All current versions of Microsoft Windows (e.g. Windows*  
> *NT, XP, 2000) and Windows Server 2003.*

>  
> *Potential Impact*  
> *This critical flaw allows an attacker to gain control of*  
> *systems via TCP Port 135. The flaw is not necessarily in*  
> *RPC, rather the flaw is in the way RPC is implemented in*  
> *Windows. When exploited, a buffer overflow is created that*  
> *could allow remote attackers to run commands with the*  
> *highest system privileges.*  
>  
> *Rating: Critical*  
> *Many networked Windows services rely on RPC in order to*  
> *communicate between machines. As a result, Microsoft ships*  
> *Windows with this service turned on by default. This means*  
> *that every Windows machine is vulnerable, unless it has*  
> *been specifically set up to not use RPC (a configuration*  
> *which may cause parts of the operating system to function*  
> *incorrectly), or unless a patch or workaround has been*  
> *applied.*  
>  
> *Protecting Against This Vulnerability*  
> *The most effective way to protect vulnerable systems is to*  
> *apply the Hotfix released by Microsoft in Security*  
> *Bulletin MS03-026. However, there is a workaround that*  
> *will disable the flawed Windows component so that an*  
> *attack over TCP Port 135 will be ineffective. According to*  
> *the Microsoft Security Bulletin, the affected service,*  
> *known as Distributed Component Object Model (DCOM), may be*  
> *disabled with little or no impact to normal Windows*  
> *functionality. The procedure for deactivating this*  
> *component consists of only a few steps, and is outlined in*  
> *the "Frequently Asked Questions" section of the Microsoft*  
> *bulletin.*  
>  
> *DCOM has long been regarded as a potential security hazard*  
> *in Windows, and best security practices recommend*  
> *disabling the service unless it is absolutely necessary.*  
> *For this reason, Retina® Network Security Scanner has*  
> *included an audit for well over a year that flags Windows*  
> *machines on which the DCOM service is running. The fix*  
> *information included within the audit instructs users to*  
> *disable DCOM using the same procedure outlined by*  
> *Microsoft.*  
>  
> *I don't know how can I deactivate DCOM service on windows*  
> *2000 advanced server platform, may somebody help me?*  
>  
> *Thank you*  
>  
> *Bijan*

--

microsoft.public.win2000.security: Re: deactivating DCOM

"Don't lose sight of security. Security is a state of being, not a state of budget. He with the most firewalls still does not win. Put down that honeypot and keep up to date on your patches. Demand better security from vendors and hold them responsible. Use what you have, and make sure you know how to use it properly and effectively."

~ Rain Forest Puppy

<http://www.wiretrip.net/rfp/txt/evolution.txt>