

DCOM RPC Vulnerabilities – NEW 9–10–2003

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2003-09/0365.html>

From: Leythos (void_at_nowhere.com)

Date: 09/11/03

Date: Thu, 11 Sep 2003 00:42:37 GMT

I got this email from my firewall company – thought you should see it:

All Versions of Windows Still Suffer from DCOM RPC Vulnerabilities

Severity: High

10 September 2003

Summary:

Today, Microsoft released a security bulletin describing three new DCOM RPC security flaws affecting most versions of Windows. The flaws consist of two buffer overflows and one Denial of Service vulnerability. An attacker could exploit the worst of the flaws to gain complete control of your Windows machines. There is no direct impact on WatchGuard products. Windows administrators should download, test, and deploy the appropriate patches immediately.

Exposure:

Remote Procedure Call (RPC) is a protocol Microsoft Windows uses to allow one computer on a network to execute a task on another computer and receive back the results of that task.

Microsoft's Security Bulletin 03–039 describes three security vulnerabilities in the DCOM RPC service that ships with Windows NT 4.0, 2000, XP, and 2003. The three flaws (two buffer overflows and one Denial of Service (DoS) vulnerability) stem from the improper handling of intentionally malformed RPC requests.

By sending a Windows machine a specially crafted RPC request, an attacker could exploit the DoS vulnerability to crash the RPC services, preventing other computers from communicating with the victim using this protocol. Worse yet, an attacker exploiting either buffer overflow flaw could gain complete control of your Windows machines!

Note: the buffer overflow vulnerabilities are very similar to the vulnerability in our July 16 alert. The recent and damaging Blaster worm exploited that particular vulnerability to infect its victims and spread all over the world. If proof of concept code is released demonstrating these new DCOM RPC flaws, virus authors may exploit these new RPC flaws

to write the next Blaster worm. You should patch immediately.

Solution Path:

Microsoft has released patches to fix these vulnerabilities. Windows administrators should download, test, and deploy the corresponding patches immediately.

Windows NT Workstation
Windows NT Server 4.0
Windows NT Server 4.0, Terminal Server Edition
Windows 2000
Windows XP
Windows XP 64 bit Edition
Windows XP 64 bit Edition Version 2003
Windows Server 2003
Windows Server 2003 64 bit Edition
For WatchGuard Firebox and SOHO Users:

In their previous DCOM RPC alert, Microsoft initially stated that attackers could exploit these RPC flaws over port 135. Researchers have since discovered a menagerie of ports attackers could exploit these flaws over, including:

TCP ports 135, 139, 445, and 593

UDP ports 135, 137, 138, 445

Both the Firebox and SOHO deny incoming access to these ports by default. As long as you have not allowed incoming access using the SMB service or custom services which include one or more of these ports, you are safe from Internet-based attackers exploiting these flaws.

For further peace of mind, Firebox users can also add these ports to their "Blocked Ports" list (Setup => Intrusion Prevention => Blocked Ports in Policy Manager) to ensure they're blocked. Although your firewall blocks these ports by default, adding them to the Blocked Ports list ensures that you don't accidentally open the ports through a service you forgot about or that someone else configured. Adding ports to the Blocked Ports list also gives you the opportunity (using a setting in the user interface) to autoblock IP addresses that attempt to connect to you on that port. (If autoblocking is new to you, see WFS 7.0's IPS Features Add More "Bounce" and read under the subhead, "Using the Firebox's Penalty Box.")

In another new development, Microsoft has also learned that administrators who've installed COM Internet Services (CIS) on their Web server are susceptible to attackers exploiting these vulnerabilities using the HTTP protocol over TCP port 80 and 443. Although the CIS package isn't installed by default, Web administrators should beware of this method of attack. Since you must allow HTTP access to your Web server (and sometimes HTTPS) in order to allow Internet users to visit your site, Web administrators should apply the corresponding patches above immediately. For more details concerning CIS and whether or not

you've installed it, see the "Frequently asked question" section of Microsoft's Security Bulletin.

--

--

spamfree999@rrOhio.com

(Remove 999 to reply to me)