Prevention, Detection & Recovery from the Windows RPC DCOM Vulnerabilities

http://securecomputing.stanford.edu/win-rpc.html
tbird65@stanford.edu
14 August 2003
Agenda

- Preventing the exploits from succeeding
  - Detecting unpatched machines
  - Installing patches
  - War stories

- Detecting compromised machines
  - Updating Norton AV signatures
  - Full disk scans
  - Manual diagnostics
Agenda cont.

- Repairing compromised machines
  - Norton
  - Manual cleaning
  - Rebuilding from scratch
RPC DCOM Vulnerability

- Microsoft MS03-026


What exploits?

Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability

August 02, 2003:

There is currently at least one autoreboot-enabled IRC bot circulating which exploits this vulnerability. At this time, the IRC bot does not appear to be automated into a worm.

August 11, 2003:

An additional exploit (kaht2.zip) has been released.

The following exploits are available:

- /data/vulnerabilities/exploits/dcomrpc.c
- /data/vulnerabilities/exploits/dcom0
- /data/vulnerabilities/exploits/DCOMExploit_UserWin92.zip
- /data/vulnerabilities/exploits/07 40 dcom48.c
- /data/vulnerabilities/exploits/06 02 dcom48.c
- /data/vulnerabilities/exploits/06 02 dcomrc_usermerklet
- /data/vulnerabilities/exploits/06 02 dcomrc
- /data/vulnerabilities/exploits/kaht2.zip
Detecting unpatched machines

- Command line tool for Windows from ISS
- Scans Class C subnets for machines without 03-026 patch

scanms
http://www.iss.net/support/product_utilities/ms03-026rpc.php
Installing patches

- IE users: http://windowsupdate.microsoft.com
- Netscape users: Start → Windows Update or on WinXP, Start → All Programs → Windows Update
- Load all critical updates
- Reboot after every update
- Return to Windows Update after each patch, until no more critical updates remain
Installing patches cont.

There are no critical updates available at this time. However, Windows Update has found other updates for your computer. To select the ones you want to install, click a category title in the list.
War Stories -- Patching

- Windows 2000
  - Microsoft says SP3 or SP4 required
  - Unofficially, patch will load on SP2, but will not be required through Windows Update (must be installed manually)
  - SP1 must be upgraded to more recent service pack
- Reboot after every critical update is applied, whether or not the system prompts you to!
War Stories – Patching cont.
Checking patches

Date: 8/5/2003  Time: 8:15:17 PM  Source: NServicePack
Event ID: 4377
Category: None
User: BRONWEN\tbird
Computer: BRONWEN

Description:
Windows XP Hotfix KB823980 was installed
For more information, see Help and Support Center at
http://go.microsoft.com/fwlink/events.asp.

Data:  Bytes  Words
Detecting Compromised Machines

- 8 exploits publicly available for DCOM vulnerability
- Stanford has experienced at least 5 different types of exploits, 2 of which are not clearly identified by Norton Anti-Virus
- Degree of danger represented by compromised machines is a matter of some debate
Updating Norton AV Sigs
Updating Norton AV Sigs cont.

LiveUpdate is searching for updates to the following Symantec products:

- AV Engine 5.0 Definitions
- AV Engine 1.5 MicroDefs
- LiveUpdate
- NAV Corporate Client NT

This could take a few minutes. Please be patient.
Full Disk Scan Options
But…

- At least one of the exploits disables Norton
- New exploits aren’t covered by AV signatures
- What are diagnostics of exploits?

http://securecomputing.stanford.edu/win-rpc.html#2
The 33571 Exploit – Win2k

- Most widespread at Stanford
- Disables Norton and other PC security applications
- Leaves a file called `update.exe` in C: drive of system (patches system)
- Reboots machine after patch installed (without knowledge of local administrator or user)
- Backdoor on port TCP/33571
Stand-alone removal tool


- Not specifically designed for 33571
- Seems to do the trick
Norton AV Will Clean

- MS Blaster & variants
- pAdmin backdoor
- IRC Cirebot backdoor

Standalone Tool Required
- the 33571 exploit
DDoS on WindowsUpdate

- MS Blaster is set to perform a distributed denial of service attack against windowsupdate.com on 16 August
- Turn your Windows systems off before you leave on Friday night!
Questions?

http://securecomputing.stanford.edu/win-rpc.html