MS03-039

Buffer Overrun In RPCSS Service Could Allow Code Execution

Briefing for Senior IT Managers

Marcus H. Sachs, P.E.
The SANS Institute
September 10, 2003

What is MS03-039?

- A bulletin from Microsoft concerning three new vulnerabilities in the Remote Procedure Call (RPC) service was published on September 10, 2003
- These vulnerabilities are **NEW** and are in addition to the ones disclosed in July
- Two of the vulnerabilities are critical – they allow for remote access at the system level, commonly known as “admin” access

SANS INSTITUTE

What happens if I do nothing?

- Most experts agree that the impact of this set of vulnerabilities is very similar to those of the previous RPC issues disclosed in July
- The MSBlaster, Nachi, and other worms seen in the past few weeks can be easily modified to spread via these new vulnerabilities
- The likelihood of a damaging worm appearing in the next few days is very high
- Remote access by a hacker is highly likely

SANS INSTITUTE

What systems are affected?

Affected Systems:

- Microsoft Windows NT Workstation 4.0
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Server 4.0, Terminal Server Edition
- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows Server 2003

Not Affected Systems:

- Microsoft Windows Millennium Edition
- Microsoft Windows 95, 98, and 98SE

SANS INSTITUTE

What can I do about it?

- The best solution is to download the proper update (patch) from Microsoft and install it on affected systems
- If that cannot be done immediately, there are two other options to mitigate the impact:
  - Block several TCP and UDP ports at the firewall
  - Disable the DCOM service on affected systems

SANS INSTITUTE

If I cannot patch, which ports should I block?

- At the firewall, block these inbound ports:
  - TCP ports 135, 139, 445, 593
  - UDP ports 135, 137, 138, 445
- Block any other ports that have been specially configured for RPC services
- If COM Internet Services or RPC over HTTP are active, then consider blocking inbound TCP and UDP ports 80 and 443

SANS INSTITUTE

What about disabling DCOM?

- The DCOM (Distributed Component Object Model) interface with the RPC service handles transactions between objects on different computers
- Disabling DCOM will remove the exposure, but will also stop other functionality such as Microsoft Outlook on a desktop computer communicating with a Microsoft Exchange server
- DCOM should only be disabled as a last resort

SANS INSTITUTE

What else do I need to know?

- In some cases, there is an additional exposure – the RPC service can be activated via a web (HTTP) command
- This is dangerous if you are only blocking the TCP/UDP ports normally used for the RPC service but leaving ports 80 or 443 open
- If the patch cannot be applied to an affected computer, then turn off the COM Internet Services (CIS) or RPC over HTTP Proxy

SANS INSTITUTE

Where do I get more information?

- The MS03-039 bulletin is available from Microsoft at:

  http://www.microsoft.com/security/security_bulletins/ms03-039.asp

- Details on updating specific operating systems are available from Microsoft at:

  http://www.microsoft.com/security/protect/default.asp

SANS INSTITUTE