

**Advisory****Title:** Potential For Significant Impact On Internet Operations Due To Vulnerability In Microsoft Operating Systems' Remote Procedure Call Server Service (RPCSS)**Date** September 10, 2003**SYSTEMS AFFECTED:** Computers using the following operating systems:

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

OVERVIEW

The National Cyber Security Division (NCSA) of the Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) Directorate is issuing this advisory in consultation with the Microsoft Corporation to heighten awareness of potential Internet disruptions resulting from the possible spread of malicious software exploiting a vulnerability in popular Microsoft Windows operating systems.

DHS believes that exploits are being developed. Two additional factors are causing heightened interest in this situation: the affected operating systems are in wide spread use, and exploitation of the vulnerability could permit the execution of arbitrary code. DHS is concerned that a properly written exploit could rapidly spread on the Internet as a worm or virus in a fashion similar to the Blaster Worm.

IMPACT

The recently announced Remote Procedure Call (RPC) vulnerability in computers running Microsoft Windows operating systems listed above could be exploited to allow the execution of arbitrary code or could cause a denial of service state in an unprotected Windows 2000 computer. Because of the significant percentage of Internet-connected computers running all affected Windows operating systems and using high speed connections (DSL or cable for example), the potential exists for a worm or virus to propagate rapidly across the Internet carrying payloads that might exploit other known vulnerabilities in switching devices, routers, or servers.

DETAILS

There are three vulnerabilities in the part of RPC that deals with RPC messages for the Distributed Component Object Model (DCOM) activation – two that would allow arbitrary code execution, and one that would result in a denial of service. These flaws result from incorrect handling of malformed messages. These particular vulnerabilities affect the DCOM interface within the RPCSS, which listens on RPC enabled ports. This interface handles DCOM object activation requests that are sent from one machine to another.

An attacker who successfully exploited these vulnerabilities could be able to run code with local system privileges on an affected system, or cause the RPCSS to fail. The attacker could be able to take any action on the system, including installing programs, viewing changing or deleting data, or creating new accounts with full privileges.

RECOMMENDATION

Due to the seriousness of the RPC vulnerability, DHS and Microsoft encourage system administrators and computer owners to take this opportunity to update vulnerable versions of Microsoft Windows operating systems as soon as possible. Additional information is available at: http://www.microsoft.com/security/security_bulletins/ms03-039.asp.

Enterprises and large organizations are encouraged to review the information in this advisory, determine its applicability to their environment and, if appropriate, block network access to the RPCSS at network boundaries. Blocking can minimize the impact of disruptive attacks originating outside the perimeter; however, it also has the potential to deny access to needed applications. The specific ports and protocols that, if applicable, should be blocked include:

TCP/135	TCP/139	TCP/445	TCP/593
UDP/135	UDP/137	UDP/138	UDP/445

If for reasons of application operability access cannot be blocked for all external hosts, DHS recommends limiting access to only those hosts that require it for normal operation. As a general rule, DHS recommends filtering all network traffic that is not required for normal operation. Sites should understand that they are accepting the risks associated if they choose to allow these ports and protocols to be accessed.

Users are encouraged to install and enable a personal firewall such as the Internet Connection Firewall in Windows XP or any firewall product for personal computers. An additional preventive step is to disable COM Internet Services (CIS) and RPC over HTTP, if applicable.

DHS encourages recipients of this Advisory to report information concerning suspicious or criminal activity to local law enforcement, local FBI's Joint Terrorism Task Force or the Homeland Security Operations Center (HSOC). The HSOC may be contacted at: Phone: (202) 282-8101.

DHS intends to update this advisory should it receive additional relevant information, including information provided to it by the user community. Based on this notification, no change to the Homeland Security Advisory System (HSAS) level is anticipated; the current HSAS level is Yellow.