



Advisory

Title: Potential For Significant Impact On Internet Operations Due To Vulnerability In Microsoft Operating Systems (2nd UPDATE: **Worm Spreading on the Internet**)

Original Date: July 24, 2003 **Updated:** July 30, 2003

Updated: August 12, 2003

SYSTEMS AFFECTED: Computers using the following operating systems:

Microsoft Windows NT 4.0

Microsoft Windows NT 4.0 Terminal Services Edition

Microsoft Windows 2000

Microsoft Windows XP

Microsoft Windows Server 2003

OVERVIEW

THIS IS THE SECOND UPDATE TO THE DEPARTMENT OF HOMELAND SECURITY (DHS) JULY 24, 2003 ADVISORY ON MICROSOFT OPERATING SYSTEMS. The DHS/ Information Analysis and Infrastructure Protection (IAIP) National Cyber Security Division (NCSD) 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 expects that exploits are being developed for malicious use. 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 and Microsoft are concerned that a properly written exploit could rapidly spread on the Internet as a worm or virus in a fashion similar to Code Red or Slammer. **(2nd UPDATE: MALICIOUS CODE DUBBED "MSBLAST", "LOVESAN", OR "BLASTER" BEGAN CIRCULATING ON THE INTERNET ON AUGUST 11TH. THIS WORM TAKES ADVANTAGE OF THE VULNERABILITY DISCUSSED IN THIS ADVISORY, AND CONTAINS CODE THAT WILL TARGET MICROSOFT'S UPDATE SERVERS ON AUGUST 16TH. THIS ADDITIONAL ATTACK COULD CAUSE SIGNIFICANT INTERNET-WIDE DISRUPTIONS. IT IS POSSIBLE THAT OTHER WORMS BASED ON THIS VULNERABILITY WILL BE RELEASED OVER THE NEXT FEW DAYS AS "COPY CAT" ATTACKS.)**

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 computer. Because of the significant percentage of Internet-connected computers running 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 is a vulnerability in the part of RPC that deals with message exchange over TCP/IP. The vulnerability results from the handling of malformed messages. This particular vulnerability

affects a Distributed Component Object Model (DCOM) interface with RPC, which listens on RPC enabled ports. This interface handles DCOM object activation requests that are sent by client machines (such as Universal Naming Convention (UNC) paths) to the server. An attacker who successfully exploited this vulnerability would be able to run code with local system privileges on an affected system. The attacker would 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. Microsoft updates, workarounds, and additional information are available at

<http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp>

DHS and Microsoft further suggest that Internet Service Providers and network administrators consider blocking TCP and UDP ports 135, 139, and 445 for inbound connections unless absolutely needed for business or operational purposes. **(2nd UPDATE: DHS RECOMMENDS THAT THE MICROSOFT UPDATE BE APPLIED AS SOON AS POSSIBLE TO THE SYSTEMS LISTED ABOVE. IN ADDITION TO BLOCKING THE TCP AND UDP PORTS LISTED ABOVE, DHS FURTHER RECOMMENDS THAT PORTS 69 (TFTP) AND 4444 BE BLOCKED WHERE POSSIBLE. BOTH OF THESE PORTS ARE USED FOR SPREADING THE WORM.)**

Advisories recommend the immediate implementation of protective actions, including best practices when available. DHS encourages recipients of this advisory to report information concerning suspicious or criminal activity to law enforcement, local FBI's Joint Terrorism Task Force or a DHS watch office. The DHS Information Analysis and Infrastructure Protection watch offices may be contacted at:

For private citizens and companies - Phone: (202) 323-3205, 1-888-585-9078,

Email: nipc.watch@fbi.gov;

Online: <http://www.nipc.gov/incident/cirr.htm>

For telecommunications industry - Phone: (703) 607-4950

Email: ncs@dhs.gov

For Federal agencies/departments - Phone: (888) 282-0870

Email: fedcirc@fedcirc.gov

Online: <https://incidentreport.fedcirc.gov>

DHS intends to update this alert 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) is anticipated; the current HSAS level is YELLOW.