



Advisory

Title: New version of the MS-RPC DCOM Worm infecting machines and creating Denial of Service Conditions

Date: August 18, 2003

SYSTEMS AFFECTED: Computers using the following operating systems:

Microsoft Windows NT 4.0
Microsoft Windows 2000
Microsoft Windows XP
Microsoft Windows Server 2003

OVERVIEW

A new worm that exploits the same security weakness as the Blaster worm (also known as “lovsan” or “msblast”) has been released on the Internet. This new worm, dubbed “nachi”, “welchia”, or “msblast.d” **does not** infect systems that have been updated to counter the Blaster worm in accordance with Microsoft’s instructions at <http://www.microsoft.com/security/incident/blast.asp>. This new worm will re-infect computers that are currently infected with Blaster or one of its variants. It deletes the original worm, patches the system by downloading the update from Microsoft, and replaces the original worm with itself.

IMPACT

Scanning by the new worm is causing denial of service conditions for some organizations. Full details about what the worm does after infecting a computer are not yet fully understood. There may be other malicious aspects of this worm such as the installation of back doors that allow intruders to access or control infected machines.

DETAILS

Information on the new worm is still emerging. It appears that the worm searches for any computer that has not been updated including those machines infected with the Blaster worm and its variants. After infecting a new computer, it deletes the file msblast.exe from the infected machine. The worm then attempts to download the patch for the MS-RPC DCOM vulnerability from Microsoft's update site and then re-boots the machine if the installation is successful. It has been reported that the variant then begins scanning or flooding the network with high volumes of ICMP (Internet Control Message Protocol) traffic causing network congestion which can result in denial of service conditions. This may be a symptom of the worm's propagation and not designed intentionally as a denial of service attack.

RECOMMENDATIONS

- For Home Users:
 - Complete patching of systems for the MS-RPC DCOM vulnerability immediately. Detailed directions for applying the patch for your system can be found at:

- <http://www.cert.org/advisories/CA-2003-20.html>
 - <http://www.microsoft.com/security/incident/blast.asp>
- Install the latest updates from your anti-virus vendor.
- For Network Administrators:
 - Complete patching of systems for the MS-RPC DCOM vulnerability immediately. Detailed directions for applying the patch for your system can be found at:
 - <http://www.cert.org/advisories/CA-2003-20.html>
 - <http://www.microsoft.com/security/incident/blast.asp>
 - Install the latest updates from your anti-virus vendor.
 - Continue MS-RPC DCOM mitigation strategy of blocking MS- RPC ports if possible.
 - Monitor your network for unusual levels of ICMP traffic, and traffic for port 707 also reportedly used by the worm.
 - Employ blocking strategies on border equipment. Reports have been received that the high levels of ICMP traffic have caused equipment at network borders to become congested.
 - Information is still emerging about this variant continue to monitor updates from your anti-virus vendor.

Additional References:

W32/Nachi.worm

http://vil.nai.com/vil/content/v_100559.htm

W32.Welchia.Worm

<http://www.sarc.com/avcenter/venc/data/w32.welchia.worm.html>

Worm_MSBLAST.D

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.D

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.