NIPC ADVISORY 00-044

"MStream Distributed Denial of Service Tool"

May 24, 2000

The potential represented by the "mstream" Distributed Denial of Service (DDoS) exploit is a serious and continuing threat. This advisory provides an update to a previously delivered NIPC DDoS detection tool that now allows users to identify the presence of mstream on host systems. The NIPC recommends that all computer network owners and organizations examine their systems for evidence of DDoS tools, including mstream.

The mstream DDoS exploit enables intruders to use multiple, Internet-connected systems to launch packet flooding denial of service attacks against one or more target systems. It was first discovered in late April 2000 on a compromised Linux system.

The NIPC tool (find_DDoS) detects the DDoS exploit in the following operating systems: Solaris on Sparc or Intel platforms, and Linux on Intel platforms. The tool has been designed to detect mstream as well as tfn2k client, tfn2k daemon, trinoo daemon, trinoo master, tfn daemon, tfn client, stacheldraht master, stacheldraht client, stachelddraht daemon and trn-rush client. This download is for Solaris 2.5.1, 2.6, and Solaris 7 on the Sparc or Intel platforms, and Linux on Intel platforms. The tool has not been tested on Solaris 8. Although the current configuration of mstream is not known to run on Windows 95, Windows 98, and Windows NT - based PC, certain versions of Trinoo do. Please refer to http://www.nipc.gov/warnings/alerts/1999/trinoo.htm for more information.

The following links provide tools and information for detecting DDoS exploits:

Readme
Solaris on Sparc Executable File (tar, compressed format) version 4.0
Linux on Intel Executable File (tar, compressed format) version 4.0
Solaris on Intel Executable File (tar, compressed format) version 4.0
Checksums (The MD5 Checksums are provided to verify the integrity of the files.)

Alternatively, specific technical instructions are available from CERT Coordination Center, SANS Institute, and other competent sources. CERT/CC, SANS Institute, and the University of Washington have published information on distributed denial of service exploits that can be readily found at the following web sites:

http://cert.org/reports/dsit_workshop.pdf
http://www.sans.org/dosstep/index.htm
http://www.staff.washington.edu/dittrich/misc/ddos/elias.txt

Recipients are asked to report significant or suspected criminal activity to their local FBI office or the NIPC Watch and Warning Unit, and to computer emergency response support and other law enforcement agencies, as appropriate. The NIPC Watch and Warning Unit can be reached at (202) 323-3204/3205/3206, or nipc.watch@fbi.gov.