NIPC ADVISORY 00-042

"Buffer Overrun Vulnerability in Kerberos Authentication Protocol"

May 17, 2000

The security experts from the Massachusetts Institute of Technology (MIT) and CERT Coordination Center have identified a serious vulnerability in some of the implementations of the Kerberos authentication protocol. This vulnerability was publicly disclosed on Bugtraq. A vulnerability has been found in Kerberos 4, and in Kerberos 5 which contains backwards compatibility with Kerberos 4. Intruders may gain root access over the network or locally by exploiting this vulnerability. The identified problem involves a buffer overrun in the krb_rd_req() function, a function that is essential to Kerberos-authenticated services using Kerberos 4. These include:

MIT Kerberos 5 releases,
MIT Kerberos 4 releases with Patch 10 and possibly earlier releases,
KerbNet running Cygnus implementation of Kerberos 5, and
Cygnus Network Security running Kerberos 4.

Daemons and services that may use the krb_rd_req() function for authentication are listed below. An intruder can remotely or locally exploit any of them to gain root access including:

Krshd,
Klogind (if Kerberos 4 authentication is used),
Telnetd (if Kerberos 4 authentication is used),
Ftpd (if Kerberos 4 authentication is used),
Rkinitd, and
Kpopd.

Patches are available for the MIT implementation at web.mit.edu/kerberos/www/.

NIPC advises recipients who use the referenced Kerberos products to consult frequently the CERT Coordination Center at www.cert.org and MIT at web.mit.edu/kerberos/www/ for additional information on this vulnerability and patches. FBI/NIPC requests recipients immediately report information on any actual or attempted use of this exploit to the local FBI office or NIPC Watch and Warning Unit at 202-323-3204/05/06.