NIPC ADVISORY 00-060

"E-Commerce Vulnerabilities"

December 01, 2000

Based on FBI investigations and other information, the NIPC has observed that there has recently been an increase in hacker activity specifically targeting U.S. systems associated with e-commerce and other Internet-hosted sites. The majority of the intrusions have occurred on Microsoft Windows NT systems, although Unix based operating systems have been victimized as well. The hackers are exploiting at least three known system vulnerabilities to gain unauthorized access and download propriety information. Although these vulnerabilities are not new, this recent activity warrants additional attention by system administrators. In most cases, the hacker activity had been ongoing for several months before the victim became aware of the intrusion. The NIPC strongly recommends that all computer network systems administrators check relevant systems and apply updated patches as necessary. Specific emphasis should be placed on systems related to e-commerce or e-banking/financial business. The following types of exploits have been observed:

Unauthorized Access to IIS Servers through Open Database Connectivity (ODBC) Data Access with Remote Data Service (RDS):

Systems Affected: Windows NT running IIS with RDS enabled.
Details: Microsoft Security Bulletin MS99-025, NIPC CyberNotes 99-22

http://www.microsoft.com/technet/security/bulletin/ms99-025.asp,
or http://www.nipc.gov/warnings/advisories/1999/99-027.htm
http://www.nipc.gov/cybernotes/cybernotes.htm

Summary: This vulnerability allows a malicious remote user to use a web browser to force a Windows NT server to return information from Structured Query Language (SQL) databases or to run system commands.

SQL Query Abuse Vulnerability

Affected Software Versions: Microsoft SQL Server Version 7.0 and Microsoft Data Engine(MSDE)1.0
Details: Microsoft Security Bulletin MS00-14, NIPC CyberNotes 20-05

http://www.nipc.gov/cybernotes/cybernotes.htm
http://www.microsoft.com/technet/security/bulletin/ms00-014.asp

Summary: This vulnerability could allow the remote author of a malicious SQL query to take unauthorized actions on a SQL Server or MSDE database.

Registry Permissions Vulnerability

Systems Affected: Windows NT 4.0 Workstation, Windows NT 4.0 Server
Details: Microsoft Security Bulletin MS00-008, NIPC CyberNotes 20-08 and 20-22

http://www.microsoft.com/technet/security/bulletin/ms00-008.asp
http://www.nipc.gov/cybernotes/cybernotes.htm

Summary: Users can modify certain registry keys such that:

- a malicious user could specify code to launch a systems crash

- a malicious user could specify code to launch at next login
- an unprivileged user could disable security measures

The NIPC is conducting further analysis of this hacker activity and will provide additional information as it becomes available.

Please report any illegal or malicious activities to your local FBI office or the NIPC, and to your military or civilian computer incident response group, as appropriate. Incidents may be reported online at http://www.nipc.gov/incident/cirr.htm**.**