NCUA INFORMATION TECHNOLOGY SECURITY ALERT

NATIONAL CREDIT UNION ADMINISTRATION
1775 DUKE STREET, ALEXANDRIA, VA 22314

DATE: June 11, 2003

TO: All Federal and State Credit Unions
All Corporate Credit Unions
All State Supervisory Regulators
All Credit Union Information Technology Vendors

SUBJECT: *BugBear.B* Worm Vulnerability Alert

PURPOSE

This alert is intended to raise awareness of an Internet worm, *BugBear.B*, that recently surfaced as a potential threat specifically targeted to financial institutions and to prompt credit unions and credit union technology service providers to take immediate steps to mitigate the threat to their organizations and customers.

BACKGROUND

Computer-based worms, viruses and Trojan horses are an increasing threat to Internet-connected systems. *BugBear.B* is a highly capable worm that specifically targets financial institutions. Credit unions with the capability to access the Internet may be vulnerable to *BugBear.B* and should institute appropriate measures to mitigate the risks posed to their servers, desktops, notebooks, and other computing devices.

Information about *BugBear.B* is available from many sources, including FedCIRC, CERT/CC, and commercial anti-virus vendors. Although the available information varies, and may be subject to change, *BugBear.B* seems to possess the following general characteristics:

- Disables security software such as anti-virus software;
- Installs spyware such as a keystroke logger and a remote control program;
- Captures keystrokes to obtain authentication information, gathers other potentially sensitive information, and e-mails it outside the institution;
- Collects and uses e-mail addresses to further distribute the worm from the infected machines; and
- Targets more than 1,300 specific financial institutions by including their Internet addresses in the worm's code.

The disabling of security software is a concern because the victim loses the protection and audit trail provided by this software. The insertion of spyware, combined with the e-mail distribution of the resulting information, could provide an attacker with confidential information such as usernames and passwords to credit union systems and accounts. With such information, the attacker could insert new malicious software or steal confidential information and/or funds. Additionally, the remote control features appear to be available to anyone who wishes to use them. Access to these features increases the risk from internal and external attackers.

The disabling of security software, insertion of spyware, and e-mailing of information could occur whether or not a credit union is included in the 1,300 specifically mentioned financial institution Internet addresses in the *BugBear.B* code.

RESPONSE TO THIS THREAT

Credit unions should review their capabilities to prevent, detect, and respond to *BugBear.B* consistent with the guidance provided in *Federal Financial Institution Examination Council's Information Technology Handbook. The Handbook is available at http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.* Specific actions may include:

- Increasing awareness among system users so they can help identify and stop the spread of computer worms and viruses;
- Ensuring anti-virus software is installed on all servers and clients with updated anti-virus signatures;
- Contacting service providers and other vendors to ensure appropriate awareness and response;
- Installing specific intrusion detection system signatures;
- Following-up closely on abnormal system and printer behavior;
- Changing passwords on potentially compromised systems;
- Following-up rigorously any suspected infection;
- Verifying configurations and patch levels; and
- Updating the information security program to address any new threats or controls.

In the event your institution is a victim of *BugBear.B*, you should report the incident to law enforcement and file a Suspicious Activity Report, as appropriate, based on the impact of the worm on your institution.

_____/s/_____
J. Leonard Skiles
Executive Director
National Credit Union Administration