The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 14458

February 12, 2002

SEC RECEIPT OF NIPC STATEMENT CONCERNING POTENTIALLY SERIOUS VULNERABILITIES IN AN INTERNET SOFTWARE PROTOCOL

URGENT/ACTION REQUESTED [14458] February 12, 2002 TO: TECHNOLOGY ADVISORY COMMITTEE No. 1-02 PRIMARY CONTACTS - MEMBER COMPLEX No. 9-02 RE: SEC RECEIPT OF NIPC STATEMENT CONCERNING POTENTIALLY SERIOUS VULNERABILITIES IN AN INTERNET SOFTWARE PROTOCOL The Securities and Exchange Commission has received the attached message from the National Information Protection Center (NIPC) concerning potentially serious vulnerabilities in a widely-used Internet software protocol. Securities market participants are urged to follow the practices outlined below to protect the integrity of their information systems and safeguard customer information. The SEC has asked us to distribute this statement to our members and has requested that firms do not publicly disseminate it. Please ensure that the appropriate persons in your firm receive this information. NIPC Statement: We are tracking vulnerabilities in an underlying Internet software protocol called Simple Network Management Protocol (SNMP) version 1. SNMPv1 is widely used and the number of potentially affected products is extensive and so far not fully identified. Routers, switches, servers, and firewalls are a few examples of technologies that rely on SNMP. We will keep you apprised of actionable information as it develops. In the meantime, we strongly encourage you to consider taking the following "best practice" steps as recommended in draft form by CERT/CC: 1. Review what versions of SNMP are running; prepare to apply patches when available. 2. Turn off SNMP traffic, if the router is not critical. 3. Block packets (e.g., SNMP) on the borders to the network (both in and out). 4. Change community strings, if the default strings are configured as community strings. 5. Use Virtual Private Network for mission critical functions. 6. Apply anti-spoof filtering. 7. Apply egress filtering to detect system compromise. 2 8. Apply recent patches for buffer overflows. In addition, the NIPC is requesting comment if you have evaluated the validity and/or extent of SNMPv1 (port 161) vulnerabilities; if you are aware of any active exploits; and, if you have comment on the utility of the above recommendations. Comment can be provided directly to the NIPC Watch and Warning Unit at (202) 323-3205, 1-888-585-9078 or nipc.watch@fbi.gov, or by using the online incident reporting form at http://www.nipc.gov/incident/cirr.htm. Donald J. Boteler Vice President - Operations Craig S. Tyle General Counsel

abridged and therefore incomplete. Communications from the Institute do not constitute, and should not be considered a substitute for, legal advice.