

# NATIONAL INFRASTRUCTURE PROTECTION CENTER

## HIGHLIGHTS

*A publication providing information on infrastructure protection issues, with emphasis on computer and network security matters.*



**Issue 1-02**  
**February 15, 2002**

*Editors:* Linda Garrison  
Martin Grand

- 
- **The Council of Europe's Convention on Cybercrime: A Global Approach to Computer Crime**
  - **SNMP Vulnerabilities: Implications for Network Security**

---

We welcome your comments and suggestions for improving this product. For more information, or to be added to the distribution list, please contact the NIPC Watch at [nipc.watch@fbi.gov](mailto:nipc.watch@fbi.gov) or call (202) 323-3204.

This issue has an overall classification of "Unclassified." This publication may be disseminated further without express permission.

### **The Council of Europe's Convention on Cybercrime: A Global Approach to Computer Crime**

*On November 23, 2001, twenty-six Council of Europe (COE) member nations, and four other nations, including the U.S., signed the COE's Convention on Cybercrime, a product of four years of work.*

#### **Escalating computer crime capabilities**

In the 1990s international consensus recognized the threat of escalating computer crime capabilities and noted the global expansion of the Internet as a facilitator of cross-border criminal actions and terrorist operations. Common provisions in laws, standard methods for computer crime investigations, and increased cooperation in cross-border investigations were clearly needed. The COE, with participation of non-COE members, such as the U.S., Canada, Japan, and South Africa, drafted an international approach to address the need for "harmonized" provisions in computer crime laws of individual nations.

The Council released a draft of the treaty for public review and comment in April 2000. The final draft, signed on November 23, 2001, incorporated specific wording to clarify areas in which concerns had been raised regarding the scope of the Convention and the broad language used to address the individual provisions. The full text of the Convention on Cybercrime can be found on-line at <http://conventions.coe.int/treaty/EN/Treaties/html/185.htm>.

#### **Benefits to the U.S.**

The Convention standardizes approaches to computer crime. The U.S. Department of Justice considers the central provisions of the Convention as being consistent with the existing framework of U.S. law and procedures. Consequently, the U.S. has much to gain from a strong, well-crafted multilateral instrument that removes or minimizes many procedural and jurisdictional obstacles that can delay or endanger international investigations and prosecutions of computer-related crimes.

#### **Critical Infrastructure and Enterprise Network Implications**

The COE Convention on Cybercrime offers many potential benefits. However, achieving these benefits requires understanding both of the Convention's provisions and U.S. policy. Major references explaining the Convention on Cybercrime include the following:

- The Explanatory Report (<http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>) by the COE contains detailed discussions of the meaning of the Convention's provisions.
- The U.S. Department of Justice's Frequently Asked Questions and Answers About the Council of Europe Convention on Cybercrime (Final Draft, released June 29, 2001) (<http://www.usdoj.gov:80/criminal/cybercrime/newCOEFAQs.html#note1>) explains that the

Convention on Cybercrime recognizes the principles of U.S. law.

## **SNMP Vulnerabilities: Implications for Network Security**

On February 12, 2002, the NIPC released an advisory notifying the public that multiple vulnerabilities in the Simple Network Management Protocol (SNMP) have been reported by Oulu University in Finland that could have severe implications for computer network security on a wide range of systems. SNMP enables network and system administrators to remotely monitor and configure devices (such as network bridges, routers, and firewalls) and is the most widely used protocol to manage several critical elements of the information infrastructure.

If exploited, the vulnerabilities could result in devices being shut down, becoming unstable, or allowing unauthorized, privileged access to computer systems—leading to remote exploitation or denial-of-service (DoS) attacks. The Oulu University test suite can be used to exploit these vulnerabilities without doing significant network reconnaissance and is openly available on the Internet. Hackers and other malicious groups will likely break down the Oulu University test suite in an effort to develop and refine new tools, including new worms and new methods of obtaining root access, which when exploited is a significant U.S. Federal crime.

Many organizations, particularly those that have been targeted in the past for social or economic protest reasons, or that have a history of being attacked by malicious hackers, could be targeted through this vulnerability. If so, the attacks could be more devastating than simple web page defacement or DoS attacks. The attacks could lead to a crash or total compromise of an organization's routers, bridges, switches, or other networking devices. Corporations could lose control over core functions, such as databases and network management frameworks. Without vendor patches, there is a high potential for disruption of a corporation's network infrastructure and corresponding damage to its bottom line. In addition to concerns over the potential degradation of network functions, malicious groups could unlawfully take advantage of SNMP vulnerabilities to gain knowledge of network topologies for future exploitation or compromise.

Most vendors whose products or services utilize SNMP are preparing patches or fixes to their systems. Until such patches are available, there are several steps that network operators can take to minimize the risk of an SNMP-based attack. Refer to CERT/CC homepage at <http://www.cert.org> for further guidance on remediation.