Software Engineering Institute
Carnegie Mellon University

CERT® Coordination Center
1996 Annual Report

October 1997

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM17-0052

Table of Contents

1 Introduction ii

1.1 Media Exposure iii

2 Highlights of CERT/CC Activities and Services v

2.1 Incident Response v

2.2 FedCIRC vii

2.3 Publications viii

2.3.1 Advisories viii

2.3.2 Vendor-Initiated Bulletins viii

2.3.3 CERT Summaries viii

2.4 Training viii

3 Advocacy & Community Support ix

3.1 Advocacy ix

3.2 Forum of Incident Response and Security Teams ix

3.3 Internet Engineering Task Force x

3.4 Vendor Relations x

3.5 Visitors x

Appendix A: CERT Advisories Published in 1996 xi

Appendix B: CERT Vendor-Initiated Bulletins Issued in 1996 xiv

1 Introduction

The CERT Coordination Center was formed by the Defense Advanced Research Projects Agency (DARPA) in November 1988 in response to the needs identified during an Internet security incident. Our charter is to work with the Internet community in detecting and resolving computer security incidents as well as taking steps to prevent future incidents. Our specific mission is to

- Provide a reliable, trusted, 24-hour, single point of contact for emergencies.
- Facilitate communication among experts working to solve security problems.
- Serve as a central point for identifying and correcting vulnerabilities in computer systems.
- Maintain close ties with research activities and conduct research to improve the security of existing systems.
- Initiate proactive measures to increase awareness and understanding of information security and computer security issues throughout the community of network users and service providers.

The CERT/CC is now part of the Networked Systems Survivability (NSS) Program at the Software Engineering Institute, Carnegie Mellon University. The primary goal of the NSS program is to ensure that appropriate technology and systems management practices are used to resist attacks on networked systems and to limit damage and ensure continuity of critical services in spite of successful attacks. Our main areas of activity for 1996 were security improvement, trust technology maturation, security incident handling, and information services.

Security improvement focuses on defining a security improvement model, a security improvement process, and a security improvement toolkit that are effective at protecting systems against current and emerging threats. To help organizations assess their security needs, we have developed a methodology for conducting information security evaluations. Field tests conducted in 1996 identified the following trends:

- movement to use of wide-area networks
- movement to distributed computing
- diffusion of system administration skill
- movement to improvement in products' ease of use, price, performance; little or no improvement in ease of management and secure administration

In the area of **trust technology**, we seek to improve the technical basis for identifying and preventing security flaws and for limiting the damage caused by successful attacks. Approaches that are effective at securing bounded systems (systems that are controlled by one administrative structure) are not effective at securing unbounded systems, such as the Internet. Therefore, our research concentrates on identifying software architecture and design practices that address security issues in unbounded systems. In 1996, the research group published an overview of current work in survivable systems. This paper and other information are available on the CERT Web site at http://www.cert.org/research/.

Incident response activities include developing an infrastructure that is effective at improving Internet-connected systems' resistance to attack as well as detecting and resolving attacks on those systems. Our primary concern is identifying and resolving high-impact threats and vulnerabilities, such as:

- attacks on network infrastructure
- widespread or automated attacks
- attacks that involve new vulnerabilities, techniques, tools

Our ongoing computer security incident response activities help the Internet community deal with its immediate problems while allowing us to understand the scope and nature of the problems and of the community's needs. Our understanding of current security problems and potential solutions comes from this first-hand experience with compromised sites on the Internet and subsequent analysis of the security incidents, intrusion techniques, configuration problems, and software vulnerabilities. To increase awareness of security issues and help organizations improve the security of their systems, we continue to **disseminate information** through multiple channels:

- hotline: +1 412 268-7090
- email: cert@cert.org
- mailing list: cert-advisory@cert.org
- USENET newsgroup: comp.security.announce
- World Wide Web: http://www.cert.org/

Media Exposure

Internet security issues continue to draw the attention of the media. Denial-of-service attacks (described in CERT advisory CA-96.21, *TCP SYN Flooding*,) drew the most media attention this year. On September 19, the day we published the advisory, the lead story of the CNBC news program *Inside Business* featured a discussion of the denial-of-service attacks and a live interview with a member of our technical staff. In the days following advisory publication, articles appeared in the *New York Times*, *Wall Street Journal*, *Pittsburgh Post-Gazette*, and *Newsweek*. The CERT/CC staff was interviewed for *Good Morning, America*, a television news program on the ABC network. The segment on Internet security aired in June 1996.

The CERT/CC and staff members were also filmed for "Life on the Internet," an episode of *Business Security*. The half-hour episode was shown on the Canadian Discovery Channel in December 1996 and will be broadcast on the U.S. Discovery Channel sometime in 1997.

The CERT/CC was also referred to in most major U.S. newspapers and in a variety of other publications, including

- *Chronicle of Higher Education*
- *Communications Week*

- *Computer World*
- *Financial Times*
- *IEEE Computer*
- *Information Management and Computer Security*
- *InformationWeek*
- *LAN Times*
- *Network Computing*
- *Telecommunications*

2 Highlights of CERT/CC Activities and Services

2.1 Incident Response

From January through December 1996, the CERT Coordination Center received 31,268 email messages and 2,062 hotline calls reporting computer security incidents or requesting information. We received 345 vulnerability reports and handled 2,573 computer security incidents during this period. More than 10,700 sites were affected by these incidents. When a security breach occurs, the CERT incident response staff helps affected sites to identify and correct problems in their systems and to develop system safeguards and security policies. We coordinate with other sites affected by the same incident and, when an affected site explicitly requests, we facilitate communication with law enforcement and investigative agencies.

When we receive a vulnerability report, CERT vulnerability experts analyze the potential vulnerability, working with technology producers and vendors. We advise them of security deficiencies in their products, help them to resolve the problems, and facilitate the distribution of corrections to other response teams and to the Internet community at large.

Below, we describe some of the most serious intruder activities reported to the CERT/CC in 1996. Unfortunately, we continue to see the same problems in 1997.

- **cgi-bin / phf exploits**

  At least weekly, and often daily, we saw reports of password files being obtained illegally by intruders who exploited a vulnerability in the PHF cgi-bin script. The phf program, which is installed by default with several implementations of httpd servers, contains a weakness that can allow intruders to execute arbitrary commands on the server. The most common attack involved an attempt to retrieve the httpd server's /etc/passwd file. Once the intruders retrieved the password file, they often attempted to crack the passwords found in the file. Sample scripts for exploiting this phf vulnerability have been widely posted on the Internet.

  We were encouraged to see that many of the attacks reported at the end of the year failed (because the attacked sites had already removed the phf program). However, the steady reports of continuing attacks indicated that these phf exploits were still being widely attempted.

- **Linux exploits**

  We saw an increase this year in break-ins and root compromises of Linux machines. In some cases, the intruders installed packet sniffers. In many of these incidents, the systems were misconfigured and/or the intruders exploited well-known vulnerabilities for which CERT advisories or Linux newsgroup posts or announcements had been published.

- **Denial-of-service attacks**

  Instructions for executing denial-of-service attacks and programs (exploitation scripts) for implementing such attacks were widely distributed this year. After this information was published, we noticed a significant and rapid increase in the number of denial-of-service attacks executed against sites. Intruders created TCP half-open connections, easily accomplished with IP spoofing. As a result, the data structure of the victim's server filled up, rendering the system unable to accept new incoming connections. Network service providers were often the targets for these attacks.

Other serious activities reported to the CERT/CC in 1996 are those we saw in 1995 as well, and continue to see in 1997.

- **Attacks on known vulnerabilities**

  We regularly received reports of systems that were compromised by intruders who gained unauthorized access to root or other privileged accounts by exploiting widely known security vulnerabilities on systems that did not have appropriate patches installed and/or systems that were running old (unpatched) versions of the operating system. Intruders continued to use automated tools to probe for known vulnerabilities. For example, intruders used automated tools to scan sites for NFS and NIS vulnerabilities. They then used the information collected to compromise vulnerable computers.

- **Packet sniffers**

  Intruders continued to install packet sniffers on root-compromised systems. These sniffers, used to collect account names and passwords, were frequently installed as part of a widely-available kit that also replaced common system files with Trojan horse programs. These kits provided "cookbook" directions that even novice, unskilled intruders could use to compromise systems. The Trojan horse binaries (du, ls, ifconfig, netstat, login, ps, and others) hid the intruders' files and sniffer activity on the system on which they were installed.

- **IP spoofing**

  We continued to receive several reports each week of IP spoofing attacks. Intruders attacked by using automated tools that are becoming widespread on the Internet. Some sites incorrectly believed that they were blocking such spoofed packets, and others planned to block them but had not yet done so.

- **Sendmail attacks**

  Intruders continued to attack the sendmail program. Unfortunately, some of these attacks were successful because sites were running old versions of sendmail and/or were not restricting the sendmail program mailer facility. The most current version of sendmail contains many security fixes.

Sendmail's program mailer facility can be restricted by using the sendmail restricted shell program (smrsh) or a program called mail.local. This year, the CERT/CC published three advisories relating to sendmail vulnerabilities.

This year, there was an increase in reports of problems that are outside the scope of the CERT/CC mission to address network security issues and improve the security of the Internet. We did, however, provide several pointers to help victims address their problems.

- **Software piracy**

  We received frequent reports this year about compromised accounts and/or poorly configured anonymous FTP servers that were being used for exchanging pirated software. News of illegal collections of software circulates quickly within the intruder community, which focuses unwanted attention on the site used for software piracy. Although software piracy is beyond the scope of the CERT/CC mission, the compromised accounts are a separate security issue. The CERT/CC staff wrote a *tech tip* about how to configure anonymous FTP service.

- **Misuse of email**

  Similarly, we saw in 1996 a large increase in the number of reports concerning email spoofing, bombing, and spamming. Although these are not considered network security problems, the CERT/CC staff did write *tech tips* discussing these email problems.

- **Viruses**

  Reports of viruses, both real and hoaxes, increased this year. Viruses, though they may be transmitted over a network, are generally outside the current scope of our Internet security work. However, we have provided pointers to virus information in our FAQ (frequently asked questions.)

2.2 FedCIRC

FedCIRC, the Federal Computer Incident Response Capability, was established in 1996 as a joint effort of the National Institute of Standards and Technology (NIST), the CERT Coordination Center, and the Computer Incident Advisory Capability (CIAC). FedCIRC provides incident response and other security-related services to Federal civilian agencies.

Information about FedCIRC is available from http://csrc.nist.gov/fedcirc/.

Agencies can contact FedCIRC by sending email to fedcirc@fedcirc.nist.gov or calling the FedCIRC hotline at 412-268-6321.

2.3 Publications

2.3.1 Advisories

The CERT/CC published 27 advisories in 1996. Among the criteria for developing an advisory are the urgency of the problem, potential impact of intruder exploitation, and existence of a software patch or workaround. On the day of release, we send advisories to a mailing list and post them to the USENET newsgroup comp.security.announce.

The archive can be also be reached through the CERT Web server at http://www.cert.org/. To keep advisories current, we update them as we receive new information. A complete listing of the advisories issued during 1996 can be found in Appendix A.

2.3.2 Vendor-Initiated Bulletins

CERT vendor-initiated bulletins contain verbatim text from vendors describing security problems and their solutions. Through these bulletins, we help the vendors' security information get wide distribution quickly. The bulletins are distributed through the same channels as advisories.

Twenty bulletins were published in 1996. Appendix B contains a complete listing.

2.3.3 CERT Summaries

We publish the CERT Summary as part of our ongoing efforts to disseminate timely information about Internet security issues. Six summaries were issued in 1996. The primary purpose of the summary is to call attention to the types of attack currently being reported to the CERT incident handling staff. Each summary includes pointers to advisories or other publications that explain how to deal with the attacks. Each summary also contains a list of new and updated files available through the World Wide Web. Summaries are distributed in the same way as advisories and bulletins.

2.4 Training

The one-day course, Internet Security for System and Network Administrators, was presented nine times this year, four times at the SEI and five at other locations (in San Francisco and Washington, D.C., and at the Defense Logistics Agency, PREPnet Security Day, and the USENIX Security Symposium). The course focuses on fundamental security practices for UNIX system administration and TCP/IP network administration. Course dates for 1997 can be found on the CERT Web site.

The CERT/CC held a three-day workshop, Incident Handling for Managers, to provide information and advice on building and managing an incident response capability.

3 Advocacy & Community Support

The CERT staff engages in a variety of activities to increase the Internet community's awareness of security issues. Our first-hand experience with security problems enables us to suggest pragmatic steps for improving the security of the attendees' systems; and, ultimately, their increased awareness will lead them to expect products with improved security characteristics. This change in customer attitude is necessary to give technology producers and vendors the incentive they need to invest in improving the security attributes of their products. A sample of these activities is in Appendix C.

3.1 Advocacy

On June 5, 1996, the manager of the NSS Program and CERT/CC testified before the U.S. Senate Governmental Affairs Committee, Permanent Subcommittee on Investigations, which is investigating the security of U.S. information systems. The information he provided includes recent trends: the increasing damage caused by intrusions, more knowledgeable intruders, increased use of automated attack tools, and a 2000% increase in computer incidents handled by the CERT Coordination Center since its establishment in 1988.

Staff members served as cluster coordinators for the High Assurance/Real-Time Cluster of the DARPA Evolutionary Design of Complex Software (EDCS) program. *Clusters* are groups of similar projects that have a basis for collaborative activities. The cluster coordinators facilitate the activities, help foster collaboration, and help plan future efforts.

A presentation to Department of Justice security contacts included discussion of current security incidents on the Internet, the changes in intruder expertise over time, and issues the security experts should address.

A member of our staff spent the fall semester as visiting faculty at Embry-Riddle Aeronautical University. He taught software engineering to graduate students and worked with the university's industrial affiliates and representatives of local industries to raise their awareness about network security and survivability.

3.2 Forum of Incident Response and Security Teams

Members of the CERT/CC staff participated in the annual FIRST (Forum of Incident Response and Security Teams) Workshop held on July 28-August 1, 1996, in Santa Clara, California, USA. Contributions included a role-playing demonstration of incident response, a tutorial on starting an incident response team, presentations on the CERT Coordination Center vulnerability analysis and advisory development processes, an update on our incident response statistics, and participation on panels. CERT/CC members were also involved in the technical colloquia held by the Forum of Incident and Security Response Teams in March and October. The colloquia are informal gatherings of technical incident response team personnel for the exchange of technical information relevant to day-to-day team operation, interaction, and coordination. A CERT/CC staff member serves on the

FIRST Steering Committee. The committee, which has always included a representative from the CERT Coordination Center, meets quarterly and holds teleconferences each month in which there is no meeting.

A current list of FIRST members is available from http://www.first.org/. As of January 1997, 59 teams belonged to FIRST, and membership applications for additional teams were pending.

3.3 Internet Engineering Task Force

Staff members regularly attended this year's meetings of the Internet Engineering Task Force (IETF). One staff member chairs two working groups, which met during the meetings. One working group is revising the IETF site security handbook for system and network administrators, which is ready for publication. The other group is drafting guidelines for security incident response teams and technology vendors.

3.4 Vendor Relations

CERT/CC has continued to work closely with technology producers to inform them of security deficiencies in their products and to facilitate and track their response to these problems. Staff members have worked to influence the vendors to improve the basic, as shipped, security within their products and to include security topics in their standard customer training courses. We interact with more than 40 vendors, as well as developers of freely available software such as sendmail and BIND. Vendors often provide information to the CERT/CC for inclusion in advisories. We summarize that information in an appendix for the benefit of the vendors' customers.

3.5 Visitors

The CERT Coordination Center hosted visits from newly formed incident response teams from Finland, Spain, and Brazil. Members of those teams spent a day getting advice on setting up a team, defining policies and procedures, and collecting statistics. In addition, the CERT/CC staff visited CERT-NL, the response team for the Netherlands and met with DFN-CERT, the German team, as well as several teams from the United States. During these meetings, technical, research, and procedural information was exchanged.

These visits are part of our effort to strengthen the worldwide incident handling infrastructure. We have found that visits such as this are vital to inter-team cooperation, enabling geographically dispersed teams to build trusting relationships and establish increasingly effective ways to cooperate and share workloads.

Appendix A: CERT Advisories Published in 1996

The following advisories were published in 1996. We update the advisories as necessary.

CA-96.01 UDP Port Denial-of-Service Attack
This advisory describes UDP port denial-of-service attacks, for which an exploitation script has been publicly posted. The advisory includes a workaround.

CA-96.02 BIND Version 4.9.3
This advisory provides information about version 4.9.3 of BIND and the vulnerabilities it addresses. The advisory appendix contains information from vendors.

CA-96.03 Vulnerability in Kerberos 4 Key Sever
This advisory describes a problem with the Kerberos 4 key server, points to patches, and provides vendor information.

CA-96.04 Corrupt Information from Network Servers
This advisory describes a vulnerability in network servers that can lead to corrupt information. The advisory includes information on subroutines for validating host names and IP addresses, patches for sendmail, and the status of vendor activity relating to the problem.

CA-96.05 Java Implementations Can Allow Connections to an Arbitrary Host
This advisory describes a vulnerability in the Netscape Navigator 2.0 Java implementation and in Release 1.0 of the Java Developer's Kit from Sun Microsystems, Inc. Workarounds and pointers to a patch are included.

CA-96.06 Vulnerability in NCSA/Apache CGI example code
This advisory describes a problem with example CGI code, as found in the NCSA 1.5a-export and APACHE 1.0.3 httpd, and possibly previous distributions of both servers. Workarounds are provided.

CA-96.07 Weaknesses in Java Bytecode Verifier
This advisory describes a vulnerability in the Java bytecode verifier portion of Sun Microsystems' Java Development Kit (JDK) 1.0 and 1.0.1. Workarounds are provided for this product and Netscape Navigator 2.0 and 2.01, which have the JDK built in.

CA-96.08 Vulnerabilities in PCNFSD
This advisory describes a vulnerability in the pcnfsd program (also known as rpc.pcnfsd). A patch is included.

CA-96.09 Vulnerability in rpc.statd
This advisory describes a vulnerability in the rpc.statd (or statd) program that allows authorized users to remove or create any file that a root user can. Vendor information is included.

CA-96.10 NIS+ Configuration Vulnerability
This advisory was originally released as AUSCERT advisory AA-96.02a. It describes a vulnerability and workarounds for versions of NIS+ in which the access rights on the NIS+ passwd table are left in an unsecure state.

CA-96.11 Interpreters in CGI bin Directories
This advisory warns users not to put interpreters in a Web server's CGI bin directory and to evaluate all programs in that directory.

CA-96.12 Vulnerability in suidperl
This advisory describes a vulnerability in systems that contain the suidperl program and that support saved set-user-ID and saved set-group-ID. Patch information is included.

CA-96.13 Vulnerabilities in the dip program
This advisory describes a vulnerability in the dip program, which is shipped with most Linux systems. Other UNIX systems may also use it. Pointers to dip 3.3.7 are included.

CA-96.14 Vulnerability in rdist
** This advisory supersedes CA-91:20 and CA-94:04. ** It describes a vulnerability in the lookup subroutine of rdist, for which an exploitation script is available. Vendor information and a pointer to a new version of rdist are included.

CA-96.15 Vulnerability in Solaris 2.5 KCMS programs
This advisory describes a vulnerability in the Solaris 2.5 kcms programs and suggests a workaround.

CA-96.16 Vulnerability in Solaris admintool
This advisory describes a vulnerability in the Solaris admintool and gives a workaround.

CA-96.17 Vulnerability in Solaris vold
This advisory describes a vulnerability in the Solaris volume management daemon (vold) and gives a workaround.

CA-96.18 Vulnerability in fm_fls
This advisory reports a configuration problem in the floating license server for Adobe FrameMaker (fm_fls). A workaround is provided.

CA-96.19 Vulnerability in expreserve
** This advisory supersedes CA-93:09 and CA-93:09a. ** It provides information about a vulnerability in the expreserve utility. A workaround and vendor information are included.

CA-96.20 Sendmail Vulnerability
This advisory describes a vulnerability in all versions of sendmail prior to 8.7.6, and includes a workaround and patch information.

CA-96.21 TCP SYN Flooding
** This advisory supersedes the IP spoofing portion of CA-95:01. ** It describes

denial-of-service attacks through TCP SYN flooding and IP spoofing. Advice about filtering is included.

CA-96.22 Vulnerabilities in bash
This advisory addresses two problems with the GNU Project's Bourn Again SHell (bash): one in yy_string_get() and one in yy_readline_get().

CA-96.23 Vulnerability in WorkMan
This advisory describes a vulnerability in the WorkMan compact disc-playing program that affects UNIX System V Release 4.0 and derivatives and Linux systems.

CA-96.24 Sendmail Daemon Mode Vulnerability
It describes a security problem relating to the daemon mode in sendmail 8.7 through 8.8.2. The advisory also includes a note about two vulnerabilities in versions 8.8.0 and 8.8.1; these have been fixed as well.

CA-96.25 Sendmail Group Permissions Vulnerability
The advisory describes a security problem affecting sendmail version 8 relating to group-writable files. Vendor patches and a workaround are included.

CA-96.26 Denial-of-Service Attack via ping
This advisory describes a denial-of-service attack using large ICMP datagrams issued via the ping command. Vendor information is included.

CA-96.27 Vulnerability in HP Software Installation Programs
This advisory describes a vulnerability in Hewlett-Packard SD-UX that may allow local users to gain root privileges. A workaround is included.

Appendix B: CERT Vendor-Initiated Bulletins Issued in 1996

The following vendor-initiated bulletins were published in 1996. Vendors publish many more bulletins than these. The CERT vendor-initiated bulletins contain vendor information that particularly warrants the widespread dissemination that CERT/CC provides.

VB-96.01 Newest version of splitvt
Vulnerability information on splitvt versions lower than 1.6.3, locations of the latest version (1.6.3), and an interim workaround to apply until you can install that version.

VB-96.02 Incorrect Permissions on Packing Subsystem
Vulnerability information on the *ATT Packaging Utility* and security measures to take on all SGI systems running IRIX 5.2, 5.3, 6.0, 6.0.1, and 6.1.

VB-96.03 Installation scripts in several SunSoft demo CDs
Vulnerability information and workaround for a potential security weakness on some SunSoft demo CDs for Catalyst CDWARE; SunSoft Developer CD, Premiere Issue; and Business Solutions.

VB-96.04 BSD/OS 2.0/2.0.1 kernel vulnerability
Information about a vulnerability in the BSD/OS 2.0/2.0.1 kernel and a pointer to the patch.

VB-96.05 OSF/1 dxconsole vulnerability
Advisory from Digital Equipment about a potential security vulnerability with dxconsole for OSF/1 V2.0 thru V3.2C and pointers to patches.

VB-96.06 unauthorized access via mount_union/mount_msdos (vfsload)
Information about a problem in FreeBSD versions 2.0 through 2.2-CURRENT, related to unauthorized access via mount_union / mount_msdos (vfsload).

VB-96.07 system stability compromise via mount_union program
Information about a problem in FreeBSD versions 2.0 through 2.2-CURRENT, related to unauthorized access via mount_union / mount_msdos (vfsload).

VB-96.08 IRIX 5.3, 6.1, 6.2 Desktop Permissions
Panel Information about a vulnerability in the IRIX 5.3, 6.1, and 6.2 operating systems regarding the permissions tool under the IRIX desktop environment.

VB-96.09 Security Compromise from Man Page Utility
Information about a vulnerability in the manual page reader for FreeBSD 2.0, 2.0.5, 2.1, 2.1-stable, and 2.2-current.

VB-96.10 Patch for kernel security issue
Information from The Santa Cruz Operation, Inc. about a problem in a kernel error handling routine. A patch is provided.

VB-96.11 Security compromise from ppp
Information from FreeBSD, Inc. on a vulnerability in the ppp program. Patch information is included.

VB-96.12 *Trojan Horse* vulnerability via rz program
Information from FreeBSD, Inc. on a Trojan horse vulnerability via the rz program. A workaround is included.

VB-96.13 Security Vulnerability in elm
Information from the Hewlett-Packard Company on vulnerabilities in the elm executable. Patch information is included.

VB-96.14 IRIX Visual Admin/User Programs
Information from Silicon Graphics Inc. about vulnerabilities in the visual admin and user tool programs used in the IRIX operating systems versions 5.2, 5.3, 6.1, and 6.2. Patch information is included.

VB-96.15 Patch for system call security issue
Information from Silicon Graphics Inc. about vulnerabilities in the visual admin and user tool programs used in the IRIX operating systems versions 5.2, 5.3, 6.1, and 6.2. Patch information is included.

VB-96.16 Solaris AFS/DFS Integrated login bug if user is in too many groups
Information from Transarc Corp. about a problem with a Solaris AFS/DFS Integrated login bug if the user is in too many groups.

VB-96.17 Linux Security FAQ Update
Linux Security FAQ Update from Alexander Yuriev. Includes information about a mount/umount vulnerability.

VB-96.18 Vulnerabilities in libc and libnsl libraries
Information from Sun Microsystems, Inc. about vulnerabilities in the libc and libnsl libraries.

VB-96.19 Possible Vulnerabilities in systour and OutOfBox
Information from Silicon Graphics Inc. about vulnerabilities in the systour and OutOfBox subsystems.

VB-96.20 Security Vulnerabilities in HP Remote Watch
Information from Hewlett-Packard Company about vulnerabilities in HP Remote Watch. These vulnerabilities allow unauthorized root access.

• Appendix C: Examples of External Events 1996

The CERT Coordination Center staff members were invited to give presentations at conferences, workshops, and meetings during 1996. This has been found to be an excellent tool to educate attendees in the area of network information system security and incident response. 1996 transition efforts included involvement in events such as these:

- Ballistic Missile Defense Organization Information Warfare Conference
- Distributed Interactive Simulation (DIS) Conference
- Fourth Annual Computer Misuse and Anomaly Detection Workshop (CMAD IV)
- LISA '96 (Large Installation System Administrators) - USENIX 10th Systems Administration Conference
- NCSA (National Computer Security Association) Firewalls and Internet Security Conference
- National Information Systems Security (NISSC) Conference
- Networld+Interop '96
- Northwestern University Security Day
- Ohio State University Security Day
- PREPnet Security Day
- SEI Software Engineering Symposium
- System Administration, Networking and Security Conference (SANS '96)
- USENIX Security Symposium
- USENIX Technical Conference
- Washington Ada Symposium
- Webmasters Conference