Software Engineering Institute
Carnegie Mellon University

CERT® Coordination Center 1997 Annual Report

January 1998

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.

This report was prepared for the

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

DM17-0052

Table of Contents

1 Introduction

The CERT Coordination Center (CERT/CC) 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 part of the Networked Systems Survivability (NSS) Program at the Software Engineering Institute (SEI), 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 1997 were security improvement, survivable network technology, security incident handling, vulnerability analysis, and information services.

Security improvement activities focus on defining a security improvement model, process, and 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. The method has been field tested with commercial organizations, financial institutions, and Internet service providers. In each case, we assessed the security of the site's network and presented our findings and recommendations to the organization's management. These provide sites with a foundation for developing an ongoing security improvement program.

The evaluation methodology is one component of the comprehensive security improvement process we are developing. Underlying the process is a framework, currently under development as well, that maps practices and technologies to security needs and identifies actions that organizations must take to ensure the survivability of their networks. We are writing a handbook to guide improvement efforts and are putting together a toolkit to assist organizations in implementing network security.

In the area of survivable network technology, we are concentrating on 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 focuses on identifying software architecture and design practices that address security issues in unbounded systems.

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:

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

2 Highlights of CERT/CC Activities and Services

2.1 Incident Response

From January through December 1997, the CERT/CC received 39,626 email messages and 1,058 hotline calls reporting computer security incidents or requesting information. We received 326 vulnerability reports and handled 2,134 computer security incidents during this period. More than 146,484 sites were affected by these incidents.

When a security breach occurs, the CERT/CC 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/CC 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.

2.1.1 Intruder Activity

Below we describe some of the most serious intruder activities reported to the CERT/CC in 1997.

1. IMAP attacks

   Throughout the year, we received reports of IMAP attacks. Intruders launched (and continue to launch) large-scale, automated scans against many networks and identify many potentially vulnerable systems. Successful IMAP attacks enable intruders to gain root-level access (super-user privileges). The CERT/CC wrote an advisory on the problem (CA-97.09). We also issued a special edition CERT Summary CS-97.04 concerning this problem.

2. Denial-of-service attacks

   This year we received more frequent and varied reports of denial-of-service attacks. Intruders are exploiting vulnerabilities addressed in various CERT advisories, and are using IP spoofing to hide the origin of the attacks. We published "Denial of Service," a tech tip that provides an overview of denial-of-service attacks and information that may help you respond to them.

Additionally, we received reports of denial-of-service attacks that are the results of an intruder creating an "UDP packet storm" either on a system or between two systems. An attack on one host causes that host to perform poorly. An attack between two hosts can cause extreme network congestion in addition to adversely affecting host performance.

3. cgi-bin exploits

CGI scripts continue to be exploited in 1997 as they were in 1996. The most frequently reported exploitation attempts involve the "phf" program. Intruders continue to use widely available "phf" exploit scripts to attempt to obtain a copy of the /etc/passwd file. Fortunately, many of the reported attempts are unsuccessful. However, intruders are now exploiting "phf" to execute a broad range of commands. As a result, they are able to add or modify files and create terminal windows.

In addition, "php" is being exploited. Similar attacks may succeed against other CGI scripts if the scripts are written without appropriate care regarding security issues. The cause of the problem is not in the CGI scripting language (such as Perl and C), but how the script is written. Advisories about CGI scripts include CA-96.06, CA-96.11, CA-97.07, CA-97.12, CA-97.24, and CA-97.25.

4. Attacks against news servers

This year, there were widespread, large-scale attacks on NNTP (Network News Transport Protocol) servers throughout the world. NNTP servers are commonly referred to as USENET news servers. Because of increased attacks, we published an advisory (CA-97.08) and a special edition CERT Summary CS-97.02.

The activity involves an attempt to exploit a vulnerability in versions of INN (InterNetNews) prior to 1.5.1. INN is a commonly used software program for serving and managing news according to the NNTP protocol. This vulnerability allows remote users to execute arbitrary commands on the news server with the same privileges as the user-id that manages the news server.

5. Root compromises

In 1997, we continued to receive daily reports of sites that have suffered root compromises. Many of these compromises can be traced to systems that are unpatched or misconfigured, which the intruders exploit using well-known vulnerabilities for which CERT advisories have been published. In the 4th quarter 1997, 13% of the incidents reported to the CERT/CC involved root compromises.

6. Linux exploits

   We continue to see incidents in which Linux machines have been the victims of root compromises. In many of these incidents, the compromised systems were unpatched or misconfigured, and the intruders exploited well-known vulnerabilities for which CERT advisories and Linux newsgroup posts or announcements have been published.

7. Increased exploitation of IRIX buffer overflows

   Buffer overflow vulnerabilities on IRIX systems are being exploited in many incidents reported to the CERT/CC. These vulnerabilities are described in a 1997 CERT advisory (CA-97.21). Vulnerable programs discussed in the advisory include df, pset, eject, login/scheme, ordist, and xlock.

8. Increased use of IRC in root compromises

   We received numerous reports that intruders are compromising machines at the root level and then installing Internet Relay Chat (IRC) clients or servers. We published an Intruder Detection Checklist that allows you to check for signs of compromise.

2.1.2 FedCIRC

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

This year FedCIRC presented a trio of summer seminars, one seminar a month during July, August, and September. Topics were Web Security and Current Trends, Connecting to the Internet Securely, and Information Security for Managers. CERT/CC staff members taught the Web Security and Current Trends and Information Security for Managers seminars. The seminars stressed the importance of employing best practices to protect Federal information resources.

Additionally, FedCIRC staff held a two-day Intrusion Detection Workshop to help Federal agencies become more effective at determining when their systems have been compromised. Topics included tools and techniques for intrusion detection, viruses and virus detection, legal issues, and practices that lead to security improvement.

On November 20-21, 1997, FedCIRC held its first Annual Workshop. The purpose of the workshop was to educate the community on current incident trends, incident detection, and incident handling.

More 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.

2.2 Incident and Vulnerability Analysis

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.

We have become a major reporting center for incidents and vulnerabilities because we have an established reputation for discretion and objectivity. Organizations trust us with sensitive information about security compromises and network vulnerabilities because we have proven our ability to keep their identities and information confidential. Our connection with the Software Engineering Institute and Carnegie Mellon University contributes to our ability to be neutral, enabling us to work with commercial competitors and government agencies without bias. As a result of the community's trust, we are able to obtain a broad view of incident and vulnerability trends and characteristics.

When we receive a vulnerability report, CERT/CC vulnerability experts analyze the potential vulnerability and work with technology producers to inform them of security deficiencies in their products and to facilitate and track their response to these problems. 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.

Another source of vulnerability information comes from incident analysis. Repeated incidents of the same type often point to the existence of a vulnerability and, often, the existence of public information or automated tools for exploiting the vulnerability.

To achieve long-term benefit from vulnerability analysis, we have begun to identify the underlying software engineering and system administration practices that lead to vulnerabilities and, conversely, practices that pre-

vent vulnerabilities. We will broadly disseminate this information to practitioners and consumers and influence educators to include it in courses for future software engineers and system administrators. Only when software is developed and installed using the defensive practices will there be a decrease in the expensive, and often haphazard, reactive use of patches and workarounds.

2.3 Publications

2.3.1 Advisories

The CERT/CC published 28 advisories in 1997. 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 and make them available on the CERT Web site at http://www.cert.org/.

To keep advisories current, we update them as we receive new information. A complete listing of advisories issued during 1997 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.

Sixteen bulletins were published in 1997. 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 1997. Two of those issues were special editions describing widespread, large-scale attacks. The primary purpose of the summary is to call attention to the types of attacks currently being reported to the CERT/CC. 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 the same way as advisories and bulletins.

2.3.4 Security Improvement Modules

This year, we published *Detecting Signs of Intrusion* and *Security for a Public Web Site*. These are the first of a new SEI document type, "security improvement modules." The two modules are available in print and on the

Web as SEI-SIM-001 and SEI-SIM-002 respectively. They are also available on the CERT Web site. We have published, in Web form only, technology-specific implementation details for the modules.

2.3.5 Other Security Information

The CERT/CC captures lessons learned from incident handling and vulnerability and makes them available to users of the Internet through a web site of security information and products. These include answers to frequently asked questions, a security checklist, "tech tips" for systems administrators, and security tools such as Tripwire, MD5, and TCP wrappers.

2.4 Media Exposure

Internet security issues increasingly draw the attention of the media. The headlines, occasionally sensational, report only a small fraction of the events that are reported to the CERT/CC. Even so, accurate reporting on security issues can raise the awareness of a broad population to the risks they face on the Internet and steps they can take to protect themselves. Ultimately, the increased visibility of security issues may lead consumers to demand increased security in the computer systems and network services they buy.

In the course of a year, the CERT/CC is referred to in most major U.S. newspapers and in a variety of other publications, from the *Chronicle of Higher Education* to *IEEE Computer*. Our staff gives interviews to a selected number of reporters, under the guidance of the SEI public affairs manager. This year we were interviewed by several computer-related publications such as *Computer Week* and *Information Week*. On January 31, 1997, *The Washington Post* published a major profile story about the CERT/CC titled "Battling Cyber Saboteurs."

This year, the CERT/CC was referred to in several major U.S. newspapers and in a variety of other publications including

- *Hotwired* (online version of *Wired Magazine*)
- *Miami Herald*
- *Computerworld*
- *PC World*
- *Aviation Magazine*
- *Byte Magazine*
- *Information Assurance Technical Analysis Center*

Three television networks interviewed staff members for news programs: MSNBC and MSNBC International; CNN News and CNN International; and NHK (Nippon Hoso Kyokai), which broadcasts "public" and educational radio and television in Japan, and provides Asia-centered international pro-

gramming to major international news organizations. Additionally, on October 15, 1997, *USA Today* named our Web site (http://www.cert.org) as one of their "hot sites."

Additionally, a CERT/CC staff member was the guest editor for a special issue of *IEEE Software* on the subject of software engineering education and co-authored one of the articles in the issue.

2.5 Training

CERT/CC staff presented "Internet Security for System and Network Administrators" six times this year. This one-day course focuses on fundamental security practices for UNIX system and TCP/IP network administration. We teach practical strategies and techniques to combat the threat of intrusions and improve the security of operating systems connected to the Internet. We include the latest information on security problems, incident trends, and defensive strategies.

2.6 Advocacy and Other Interactions with the Community

The CERT/CC has the opportunity to advocate high-level changes that improve Internet security and network survivability. Additionally, CERT/CC staff members are invited to give presentations at conferences, workshops, and meetings. These activities enhance the understanding of Internet security and incident response issues.

2.6.1 President's Commission on Critical Infrastructure Protection

In January 1997, members of the CERT/CC staff submitted a report to the President's Commission on Critical Infrastructure Protection (PCCIP). In the report we identify threats and vulnerabilities of the Internet, and we estimate the cascade effect that a successful, sustained attack on the Internet would have on critical national infrastructures such as telecommunications, banking and finance, emergency services, and the information infrastructure itself. We discuss the implications for public policy and make specific recommendations. The paper has been widely distributed and quoted. A copy of our report to the PCCIP can be found on the CERT Web site.

2.6.2 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. One group published RFC 2196, *Site Security Handbook* and *Expectations for Security Incident Response*, for which the staff member served as editor and contributing author. The *Site Security Handbook* replaces RFC 1244.

2.6.3 Internet Architecture Board

A CERT/CC staff member was one of 25 participants in an Internet Architecture Board (IAB) Security Architecture Workshop. The primary goal of the workshop was to identify what Internet security mechanism are available, and when they can, should, or must be used. Among the topics discussed were short-term guidelines for IETF working groups on improving consideration of security issues and, for the long term, an Internet security "architecture."

The IAB was established in 1983 and is a technical advisory group of the Internet Society. The IAB consists of 13 voting members. Six of the members are nominated by the IETF. The IAB exists to serve and help the IETF, attempting to strike a balance between action and reaction.

2.6.4 Forum of Incident Response and Security Teams (FIRST)

The 9th Annual FIRST (Forum of Incident Response and Security Teams) Conference was held in June in Bristol, England. The conference was attended by 159 people from 23 countries. CERT/CC staff members gave talks on hiring incident response staff, dealing with the media, and the current activities in the CERT/CC. During the conference elections were held for position on the FIRST Steering Committee. A CERT/CC staff member was elected chair of the Steering Committee. The committee, which has always included a representative from the CERT/CC, 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/team-info/. As of December 1997, 66 teams belonged to FIRST, and membership applications for additional teams are pending.

2.6.5 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.

2.6.6 Visitors

Among our visitors this year were members of JANET-CERT and UKERNA (response teams in the United Kingdom), JPCERT (a newly formed Japanese response team), DFN-CERT (the German response team), CERT-NL (the Dutch response team), AUSCERT (the Australian response team), ASSIST (a Department of Defense response team), and SingCERT (a response team from Singapore). These visits enhance understanding of Internet security and incident response issues and promote mutual trust and cooperation that are essential for effective response to international incidents.

Other visitors included the Federal Reserve Bank of New York, IBM Global Security Analysis Laboratory, researchers from the Air Force Academy, the Air Intelligence Agency, members of the Army Research Laboratory staff, Pennsylvania Congressman Michael Doyle, Naval Information Warfare Activity staff, Secunet, Microsoft, and computer expert Wieste Venema. These visits were primarily information exchanges about work we are doing in common areas.

2.6.7 External Events

The CERT/CC staff members were invited to give presentations at conferences, workshops, and meeting during 1997. This has been found to be an excellent tool to educate attendees in the are of network information system security and incident response. Transition efforts included involvement in events such as these:

- 1st Annual ACM Workshop on Education in Computer Security
- Federal Computer Security Managers Meeting
- National Coordinating Center for Telecommunications
- Security and Fraud Prevention/Electronic Banking and Security Conference
- USENIX 1997 Annual Technical Conference
- COMPASS '97, 12th Annual Conference on Computer Assurance
- Information Protection Conference (U.S. Air Force)
- SANS '97 (6th Annual System Administration, Networking, and Security Conference)
- Defense Advanced Research Projects Agency (DARPA) Intrusion Detection Principal Investigators meeting
- Enabling Technologies for Advanced Transportation Systems Roundtable
- International Arris Conference
- Software Technology and Engineering Practice (STEP) '97
- Software Engineering Institute Symposium
- USENIX LISA '97
- Network Security Information Exchange (NSIE)
- Forensic Association of Computer Technologists (FACT)
- Joint Information Assurance Operation Tools Working Group (JIAOTWG)

- Automated Software Engineering (ASE '97) 12th IEEE International Conference
- Embry-Riddle Aeronautical University Industry Advisory Board
- Working Group on Software Engineering Education and Training
- Monmouth University
- Cybercrime: Electronic Commerce & Banking; Corporate, Bank, and Computer Security; Financial Crimes & Information Warfare

Appendix A: CERT Advisories Published in 1997

The following advisories were published in 1997. We update the advisories as necessary. Advisories are available on the CERT Web site at http://www.cert.org/.

CA-97.01 **Vulnerabilities in UNIX FLEXlm**
This advisory describes multi-platform UNIX FLEXlm vulnerabilities. These problems may allow local users to create arbitrary files on the system and execute arbitrary programs using the privileges of the user running the FLEXlm daemons.

CA-97.02 **Vulnerability in newgrp(1) program**
This advisory describes a vulnerability in the newgrp(1) program under HP-UX 9.x and 10.x that may allow users to gain root privileges. A workaround is provided.

CA-97.03 **Vulnerability in csetup program**
A vulnerability in the csetup program under IRIX versions 5.x, 6.0, 6.0.1, 6.1, and 6.2 allows local users to create or overwrite arbitrary files on the system and ultimately gain root privileges. A workaround is provided.

CA-97.04 **Vulnerability in talkd(8) program**
A vulnerability in talkd(8) program used by talk(1) makes it possible to provide corrupt DNS information to a host and to remotely execute arbitrary commands with root privileges. This advisory includes information on how to solve the general problem as well as the specific one.

CA-97.05 **MIME conversion buffer overflow in sendmail versions in 8.8.3 and 8.8.4**
This advisory addresses a MIME conversion buffer overflow in sendmail versions in 8.8.3 and 8.8.4. This advisory includes information, pointers to the latest version of sendmail, a workaround, and general precautions to take when using sendmail.

CA-97.06 **Vulnerability in rlogin program**
This advisory reports a vulnerability in many implementations of the rlogin program, including eklogin and klogin. Vendor information and a workaround are included.

CA-97.07 **Vulnerability in the nph-test-cgi script**
This advisory points out a vulnerability in the nph-test-cgi script included with some http daemons. Readers are urged to disable the script. Vendor information is included.

CA-97.08 **Vulnerabilities in INN**

This advisory describes two vulnerabilities in the InterNetNews server (INN). One affects versions 1.5 and earlier; the other affects 1.5.1 and earlier. This advisory includes pointers to version 1.5.1 and earlier. Updated information on the second vulnerability was added as "Topic 2." Pointers to all relevant patches are included, along with information from vendors.

CA-97.09 **Vulnerability in IMAP and POP**

This advisory reports a vulnerability in some versions of the Internet Message Access Protocol (IMAP) and Post Office Protocol (POP) implementations (imapd, ipop2d, and ipop3d). Vendor and upgrade information are included.

CA-97.10 **Buffer overflow in libraries using Natural Language Service (NLS)**

This advisory reports a buffer overflow condition that affects some libraries using the Natural Language Service (NLS). Vendor vulnerability and patch information are included.

CA-97.11 **Buffer overflow vulnerability in Xt library**

This advisory reports a buffer overflow vulnerability in the Xt library of the X Windowing System. Vendor vulnerability and patch information are included.

CA-97.12 **Vulnerability in webdist.cgi-bin program**

This advisory reports a vulnerability in the webdist.cgi-bin program, part of the IRIX Mindshare Out Box package, available with IRIX 5.x and 6.x. By exploiting this vulnerability, both local and remote users may be able to execute arbitrary commands with the privileges of the httpd daemon. A workaround is included.

CA-97.13 **Buffer overflow problem in xlock**

This advisory reports a buffer overflow problem in some versions of xlock. This problem makes it possible for local users to execute arbitrary programs as a privileged user. Patch information and a workaround are included.

CA-97.14 **Vulnerability in metamail**

This advisory reports a vulnerability in metamail, a package that implements MIME. All versions of metamail through 2.7 are vulnerable.

CA-97.15 **Vulnerability in SGI login program**

This advisory describes a vulnerability in the SGI login program when the LOCKOUT parameter is set to a number greater than zero. The vulnerability is present in IRIS 5.3 and 6.2, and perhaps other versions.

CA-97.16 **Vulnerability in ftpd**
This advisory describes a vulnerability in some versions of ftpd distributed and installed under various UNIX platforms. Includes vendor information.

CA-97.17 **Buffer overflow in suidperl**
This advisory addresses a buffer overflow condition in suidperl (sperl) built from Perl 4.n and Perl 5.n distributions on UNIX systems. It suggests several solutions and includes vendor information and a patch for Perl version 5.003.

CA-97.18 **Buffer overflow in at(1) program**
This advisory addresses a buffer overflow condition in some versions of the at(1) program. Patch information and a workaround are provided.

CA-97.19 **Vulnerability in BSD-based lpr printing software**
This advisory describes a vulnerability in BSD-based lpr printing software. Vendor information and a pointer to a wrapper are included.

CA-97.20 **Vulnerability in JavaScript**
This advisory reports a vulnerability in JavaScript that enables remote attackers to monitor a user's Web activities.

CA-97.21 **Buffer overflow problems in SGI IRIS systems**
In this advisory, we describe 6 buffer overflow problems in SGI IRIS systems. Problems affect the df, pset, eject, login/scheme, ordist, and xlock programs. Workarounds and a pointer to a wrapper are provided.

CA-97.22 **Vulnerability in BIND**
This advisory supersedes CA-96.02. It describes a vulnerability in all versions of BIND before release 4.9.6, suggests several solutions, and provides pointers to the current version of bind.

CA-97.23 **Buffer overflow problem in rdist**
This advisory discusses a buffer overflow problem in rdist. It is a different vulnerability from the one described in CA-96.14.

CA-97.24 **Vulnerability in Count cgi**
This advisory describes a buffer overrun vulnerability which exists in the Count.cgi cgi-bin program that allows intruders to force Count.cgi to execute arbitrary commands.

CA-97.25 **Vulnerability in CGI metachar**
This advisory reports a vulnerability in some CGI scripts. This problem allows an attacker

to execute arbitrary commands on a WWW server under the effective user-id of the server process.

CA-97.26 **Vulnerability in statd (1M) program**
This advisory reports a vulnerability that exists in the statd (1M) program, available on a variety of Unix platforms.

CA-97.27 **FTP Bounce**
This advisory discusses the use of the PORT command in the FTP protocol.

CA-97.28 **IP Denial-of-Service Attacks**
This advisory reports on two IP denial-of-service attacks

Appendix B: CERT Vendor-Initiated Bulletins Issued in 1997

The following vendor-initiated bulletins were published in 1997. 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-97.01 **Division of Privilege (DoP) - Potential Security Vulnerability**
Information from Digital concerning the discovery a potential vulnerability with the Division of Privilege (DoP), "/usr/sbin/dop" for DIGITAL UNIX V4.0, V4.0A, and V4.0B, where under certain circumstances, an unauthorized user many gain unauthorized privileges. A workaround is provided.

VB-97.02 **Security Hole in Guestbook Script for Web Servers Using SSI**
Information from Selena Sol about a vulnerability in all versions of Selena Sol's Guestbook.

VB-97.03 **Vulnerability in rpcbind**
Information from Sun Microsystems, Inc. about a vulnerability in the rpcbind program, which can aid an attacker to gain unauthorized access if exploited. Patches are provided.

VB-97.04 **Security Vulnerability in chfn executable**
Information from Hewlett-Packard concerning a vulnerability with the chfn command. A patch is provided.

VB-97.05 **Vulnerability in Lynx Temporary Files**
Information about a vulnerability in Lynx 2.7.1. Patches are provided.

VB-97.06 **Vulnerability in Lynx Downloading**
Information about a vulnerability in versions of Lynx up to and including version 2.7.1 on Unix or Unix-like operating systems. A patch is provided.

VB-97.07 **IRIX webdist.cgi, handler and wrap programs**
Information from Silicon Graphics Inc. about a vulnerability with cgi-bin programs webdist.cgi, handler and wrap available for IRIX 5.x and 6.x. A patch is provided.

VB-97.08 **Vulnerability in Transarc DCE Integrated login for sites running both AFS and DCE**

Information from Transarc Corp concerning a vulnerability in Transarc DCE Integrated login for sites running both AFS and DCE. Patches are provided.

VB-97.09 **Vulnerabilities in Cisco CHAP Authentication**

Information from Cisco Systems about a vulnerability that exists in PPP CHAP authentication in all "classic" Cisco IOS software versions starting with the introduction of CHAP support in release 9.1(1) and a vulnerability that exists in Cisco IOS/700 software. Workarounds are provided.

VB-97.10 **Security bugfix for Samba**

Information from the Samba Team about a security hole in all versions of Samba. A new release of Samba is provided.

VB-97.11 **Vulnerability in "nosuid" mount option**

Information from NEC Corporation concerning a vulnerability in the "nosuid" mount option. Patches are provided.

VB-97.12 **Potential denial-of-service attack in the OSF/DCE security server**

Information from The Open Group about a potential problem in the security serve that could allow for a denial-of-service attack. A fix is provided.

VB-97.13 **Vulnerability in GlimpseHTTP and WebGlimpse CGI scripts**

Information from Project FUSE, University of Arizona concerning vulnerabilities in both GlimpseHTTP and WebGlimpse. An upgrade is available.

VB-97.14 **Vulnerability in /usr/bin/X11/scoterm**

Information from Santa Cruz Operation, Inc. about a vulnerability in the implementation of scoterm. Patches are provided.

VB-97.15 **Vulnerability in nix_cachemgr**

Information from Sun Microsystems, Inc. about a vulnerability in nix_cachemgr. Patches are provided.

VB-97.16 **CrackLib**

A bug in CrackLib v2.5 may be exploitable to obtain root privileges when logged on machines where CrackLib is installed as part of a SUID program, such as "/bin/passwd". A upgrade or patch is available.