Software Engineering Institute
Carnegie Mellon University

CERT® Coordination Center 1999 Annual Report

January 2000

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

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 1999 were survivable network management practices, survivable network technology, security incident handling, vulnerability analysis, and information services.

We develop and publish security improvement practices that provide concrete, practical guidance that helps organizations improve the security of their networked computer systems. These practices are published as security improvement modules and focus on best practices that address important problems in network security.

Development is under way for a self-evaluation method that builds on what we learned during our pilot. Self-evaluations will give organizations a comprehensive, repeatable technique they can use to identify vulnerabilities in their networked systems and keep up with changes over time. The method takes into consideration policy, management, administration, and other organizational issues, as well as technology, so organizations can gain a comprehensive view of the state of their systems' security.

Because security improvement is an ongoing process within an organization, we are developing an adaptive security management process that builds on and incorporates our work on security practices and security self-evaluations. The adaptive process presents a structure that organizations can use to develop and execute a plan for continuously improving the security of their networked systems.

In the area of survivable network technology, the CERT/CC is concentrating on the technical basis for identifying and preventing security flaws and for preserving essential services if a system is penetrated and compromised. 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, the technical approaches include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability trade-off analysis, and the development of security architectures. Drawing on our vast collection of incident data, our researchers are creating usage scenarios and intruder scenarios that will be used to identify the points in an architecture that are both essential to an organization's mission and susceptible to attack. This provides the basis for a method for analyzing network technology. Also under way is development of a simulator for modeling and predicting the survivability attributes of systems while they are under development, preventing costly vulnerabilities before the system is built.

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 1999, the CERT/CC received 32,967 email messages and 2,099 hotline calls reporting computer security incidents or requesting information. We received 419 vulnerability reports and handled 8,268 computer security incidents during this period. More than 4,387,088 hosts 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 1999.

1. **Growth and Evolution of Distributed Systems Intruder Tools**
   The CERT/CC received reports of intruders using distributed systems intruder tools (DSIT). The use of these tools was reported in an alert and an incident note (CA-99-17 and IN-99-07) and these tools were the subject of a November workshop. While not new, DSIT have grown in use and in sophistication. With DSIT, a single command from an attacker can cause several thousand concurrent attacks on one or multiple targets. Damage to systems can include those used to do the attack as well as the targeted victim. For the targeted victim the impact can be severe. For example, in a denial-of-service attack using distributed technology, the targeted system receives simultaneous attacks flooding the network normally used to communicate and trace the attacks in addition to preventing legitimate traffic from traversing the network.

2. **Virus and Trojan Horse Activity; Melissa; CIH/Chernobyl; Happy99; and ExploreZip**
   Major viruses and Trojan horse reported include; Melissa; CIH/Chernobyl; Happy99, and ExploreZip.

   Reported in CA-99-04, the Melissa virus spreads mainly as Microsoft Word 97 and Word 2000 attachments in email. Because Melissa propagates by automatically emailing copies of infected files to other users, it had the potential to cause severe problems across the Internet. In addition to its ability to cause denial of service by overloading mail systems, the virus could also cause confidential documents to be leaked without the users knowledge.

Reported in IN-99-03, the CIH (Chernobyl) virus infects executable files and is spread by executing an infected file. Since many files are executed during normal use of a computer, the CIH virus can infect many files quickly. The most common version of the virus became active on April 26, but there are other versions that become active on the 26th day of other months.

Reported in IN-99-02 and CA-99-02, Happy99.exe is a Trojan horse. The first time Happy99.exe is executed, a fireworks display saying "Happy 99" appears on the computer screen. At the same time, it modifies system files to email itself to other people.

Reported in CA-99-06, the ExploreZip program is a Trojan horse affecting Windows 95/98/NT systems. It modifies system files and destroys files. For ExploreZip to work, a person must open or run an infected email attachment, which allows the program to install a copy of itself on the victim's computer and enables further propagation. ExploreZip may also behave as a worm, propagating to other network machines without human interaction.

3. **RPC Vulnerabilities**
   In a significant number of incidents reported, intruders exploited at least one of three RPC vulnerabilities. As reported in alerts throughout the year (CA-99-05, CA-99-08, and IN-99-04) the vulnerable services are; rpc.cmsd; statd and automoutd; and ttbserverd. Exploitations of these vulnerable services can lead to root compromise.

2.1.2 Year 2000 Preparation and Operation

The CERT/CC provided a range of support and information regarding the Y2K transition.

In the months preceding Y2K, staff collaborated with technical experts around the world. Staff coordinated and led sessions at the International Y2K workshop held October 26- 28, 1999. This workshop generated three documents - an analysis paper focused on the threats posed by the transition, an FAQ on determining whether a software glitch is Y2K related or malicious activity by a potential intruder, and an incident reporting form. All three documents were further refined and published on the CERT/CC web site.

During the Y2K event, the CERT/CC maintained normal operations. Staff monitored the Internet for activity, received incident reports from affected sites, and worked with severely compromised sites to restore operations. Staff published regular reports to inform the community of activity being reported.

2.1.3 FedCIRC

The CERT/CC incident response team is part of FedCIRC, the Federal Computer Incident Response Capability. FedCIRC provides incident response and other security- related services to Federal civilian agencies. It was established in 1996 as a pilot effort of the National Institute of Standards and Technology (NIST), the CERT/CC, and the Computer Incident Advisory Capability (CIAC). As of October 1, 1998, FedCIRC is managed by the General Services Administration (GSA) and operated by the CERT/CC.

This year CERT/CC staff attended a FedCIRC Agency forum and made a presentation about its response to the Melissa virus. Staff also briefed the forum about activities and responses the CERT/CC would take to react to similar incidents in the future.

More information about FedCIRC (including guidelines for reporting an incident) is available at http://www.fedcirc.gov or by calling the FedCIRC Management Center at (202) 708-5060.

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.

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 prevent 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 17 advisories in 1999. 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, 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. The complete listing of advisories issued during 1999 can be found in Appendix A.

2.3.2 CERT Summaries

We publish the CERT Summary as part of our ongoing efforts to disseminate timely information about Internet security issues. Five summaries were issued in 1999. 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. Summaries are distributed the same way as advisories.

2.3.3 Incident and Vulnerability Notes

The CERT/CC publishes Incident Notes and Vulnerability Notes as an informal means for giving the Internet community timely information relating to the security of its sites. Incident Notes describe current intruder activities that have been reported to the CERT/CC incident response team. Vulnerability Notes describe weaknesses in Internet-related systems that could be exploited but that currently do not meet the criteria for advisories. In 1999, we published eight Incident Notes and three Vulnerability Notes. Appendices B and C contain a complete listing.

2.3.4 Survivable Network Management Practices

Practices available on the CERT web site and in hard copy include the following:

- *Detecting Signs of Intrusion*
- *Preparing to Detect Signs of Intrusion*
- *Security for Information Technology Service Contracts*
- *Responding to Intrusions*
- *Securing Network Servers*
- *Securing Desktop Workstations*
- *Deploying Firewalls*

The CERT/CC staff completed a framework for the Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE). OCTAVE is a framework for identifying and managing information security risks. It defines a comprehensive evaluation that allows an enterprise to identify the information assets that are important to the mission of the organization, the threats to those assets, and vulnerabilities that may expose the information to the identified threats.

The CERT/CC staff also completed a framework for the Adaptive Security Management (ASM) method. The ASM model provides a structure for organizations to continuously monitor and adjust the security of their enterprise. The model provides the ability to recognize the need for adjustments in security posture and supports the ability to accomplish those adjustments quickly and correctly.

2.3.5 Survivable Network Technology

Information on Survivable Network Technology activities is in the following research papers available on the CERT web site:

- *Survivable Network Systems: An Emerging Discipline*
- *A Case Study in Survivable Network System Analysis*
- *Requirements Definition for Survivable Network Systems*
- *Survivable Network Systems: A Case Study*

2.3.6 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 archive of security information. These include answers to frequently asked questions, a security checklist, and “tech tips” for systems administrators.

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, the CERT/CC was referenced in a variety of publications including; *The New York Times*; *USA Today*; *The Washington Post*; *The Wall Street Journal*; *The Boston Globe*; *San Jose Mercury News*; *CNN Financial Network (an online publication)*; *CNET News* (an online publication); *Computerworld*; *Infoworld*; and a number of other newspapers located around the country. In addition, CERT/CC operations were included in widely distributed articles from wire services such as the

Associated Press. Online media coverage included MSNBC.com, ABCnews.com, and CNN.com.

2.5 Training

CERT/CC staff provides access to ongoing training to improve the skills of incident response teams and individuals charged with information security responsibilities through seminars and courses. These offerings provide pragmatic information needed to develop an incident response capability and are based on CERT/CC experience. Training for managers of incident response teams includes topics such as team communication, interacting with the media, balancing workload, and setting priorities. Topics for the technical staff include detecting and responding to incidents, intruder trends and attack patterns, analyzing vulnerabilities, and policies and planning. Specific types of incidents are included, such as those involving UNIX, the World Wide Web, and cgi-bin scripts. This training is interactive, including role-playing to give participants experience in applying the instruction. Courses offered in 1999 included the following:

- *Concepts and Trends in Information Security*
- *Information Security for System and Network Administrators*
- *Managing Computer Security Incident Response Teams (CSIRTs)*
- *Computer Security Incident Handling for Technical Staff (Introduction)*
- *Computer Security Incident Handling for Technical Staff (Advanced)*

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 The Distributed-Systems Intruder Tools (DSIT) Workshop

On November 2-4, 1999, the CERT/CC invited 30 experts from around the world to address a category of network attack tools that use distributed systems in increasingly sophisticated ways. Intruders are maturing an attack technology that goes beyond using individual systems as the starting point for an attack. Rather, they can potentially use tens of thousands of unprotected Internet nodes together in order to coordinate an attack against selected targets. Each attacking node has limited information on who is initiating the attack and from where; and no node need have a list of all attacking systems. For the victim, the impact can be extensive.

During the Distributed-Systems Intruder Tools (DSIT) Workshop, participants discussed a large number of approaches to preventing, detecting, and responding to distributed- systems attacks. The CERT/CC specifically invited technical personnel that could contribute technically to the solutions regardless of their position in their home organization or political stature in the community. Thus, the workshop effectively provided a venue for experts around the world to share experiences, gain a common understanding, and creatively brainstorm possible responses and solutions to this category of attack before the dissemination of the attack tools – and the attacks themselves – become widespread. Further, the CERT/CC published *Results of the Distributed-Systems Intruder Tools Workshop* on its web site. The paper explains the threat posed by these intruder tools and provides suggestions for safeguarding systems from this type of malicious activity.

2.6.2 Protecting the Internet Infrastructure

In a January 1997 report to the President's Commission on Critical Infrastructure Protection (PCCIP), the CERT/CC outlined the effect of a successful, sustained attack on the Internet for critical national infrastructures such as telecommunications, banking and finance, emergency services, and the information infrastructure itself. The concerns raised there continue to be influential and guide our work in this area.

The CERT/CC assigns a higher priority to incidents and vulnerabilities that directly effect the Internet infrastructure. Toward that end, CERT/CC staff monitors reports closely for incidents that indicate a threat to infrastructure sites such as network service providers and Internet service providers. Similarly, domain name servers and routers receive close attention as vital infrastructure components. We also regularly review incident and vulnerability data for threats to the operation of widely used technology like the WWW and prevalent applications like NT, Solaris, sendmail, and Java. We also look closely at the activity reported by major archive sites and other computer security incident response teams.

In addition to its incident response work, CERT/CC staff attended and participated in a number of discussions centered around critical infrastructure protection. CERT/CC technical staff is actively involved in planning security improvements to the Domain Name Service, on which all Internet users depend. We have met with Network Solutions, Inc. and the Internet Assigned Numbers Authority (IANA), who are charged with managing much of the domain name system, and are active in the Internet Society, which also influences change in the Internet.

2.6.3 Internet Engineering Task Force

Members of our staff influence the definition of Internet protocols through participation in the Internet Engineering Task Force (IETF); a member of our staff sits on the Security Area Advisory Group to ensure that the CERT/CC perspective is brought to bear on all new standards activities.

2.6.4 Building an Incident Response Infrastructure

The scale of emerging networks and the diversity of user communities make it impractical for a single organization to provide universal support for addressing computer security issues. The CERT/CC model, from the start, presumed the creation of multiple incident response organizations, each serving a particular user group. The CERT/CC staff regularly works with sites to help them form incident response teams and provides guidance to newly formed teams. In addition, our staff completed work on the CSIRT Handbook (CMU/SEI-98-001). This document provides guidance in forming and operating a Computer Security Incident Response Team (CSIRT).

We also meet with other teams to enhance our mutual understanding of Internet security and incident response issues. We meet and work with other teams to promote the mutual trust and cooperation that are essential for effective response to global incidents.

2.6.5 Forum of Incident Response and Security Teams (FIRST)

Members of the CERT/CC participated in the 1999 Forum of Incident Response and Security Teams (FIRST) Conference.

CERT/CC staff helped lead the event and CERT/CC staff made presentations and participated in discussions with other attendees representing government, academia, and private industry. The conference drew attendees from all over the world.

A current list of FIRST members is available from http://www.first.org/team-info/. Currently, more than 80 teams belong to FIRST.

2.6.6 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 100 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.

2.6.7 Visitors

United States Senator Rick Santorum (R-PA) visited the CERT/CC and the Software Engineering Institute to gain a first-hand understanding of the mission and work.

Other visitors included a representatives of the following; Office of the Assistant Secretary of Defense, Critical Infrastructure Protection; the Defense Information Assurance Program (DIAP); the National Security Council, Global issues & Multinational Affairs; the Critical Information Assurance Office (CIAO); and the U.S. Army Reserve. These visits provide an additional means by which to obtain feedback and direction with our sponsoring organizations.

2.6.8 External Events

CERT/CC staff members were invited to give presentations and participate in conferences, workshops, and meetings during 1999. This has been found to be an excellent tool to educate attendees in the area of network information system security and incident response. Transition efforts included involvement in conferences and meetings such as the examples listed below:

- Network Security Information Exchange (NSIE)
- EuroCERT
- FIRST Technical Colloquium and FIRST Steering Committee Meeting
- 7th Annual USENIX Security Symposium
- Software Engineering Education and Training Working Group Meeting
- Conference on Software Engineering Education and Training Joint Information Assurance Tools Working Group
- DARPA Intrusion Detection Principle Investigators Workshop
- New Security Paradigms Workshop/Association for Computing Machinery
- Workshop on Information Hiding
- SEI Symposium
- Insider Misuse Workshop
- Countering Cyber-Terrorism/University of Southern California Information Sciences Institute
- Special Interest Group on Computer Science Education (SIGCSE) Conference
- Tech Trends 2000 Conference
- Internet Engineering Task Force (IETF) – Intrusion Detection Working Group (IDWG) meeting
- DARPATech 1999 Systems and Technology Symposium
- Planning Retreat for a Multi-Institutional Consortium on Critical Infrastructure Protection sponsored by the University of Idaho
- Workshop on Countering Cyber-Terrorism sponsored by the Information Sciences Institute of the University of Southern California
- IEEE Software Editorial Board Meeting
- 11th International Conference on Software Engineering and Knowledge Engineering (SEKE 1999)
- International Conference on Software Engineering
- 1999 Forum of Incident Response and Security Teams (FIRST) Conference

Appendix A: CERT Advisories

Published in 1999 The following advisories were published in 1999. We update the advisories as necessary. Advisories are available on the CERT Web site at http://www.cert.org/.

CA-99.01
Trojan Horse Version of TCP Wrappers
TCP Wrappers is a tool commonly used on Unix systems to monitor and filter connections to network services. The Trojan horse version of TCP Wrappers provides root access to intruders initiating connections which have a source port of 421. Additionally, upon compilation, this Trojan horse version sends email to an external address. This email includes information identifying the site and the account that compiled the program. Specifically, the program sends information obtained from running the commands 'whoami' and 'uname -a'.

CA-99.02
Trojan Horses
Trojan horses included in this alert included a false upgrade to Internet Explorer, a version of util-linux, the version of TCP Wrappers described in CA-99.01, and a list of Trojan horses previously published.

The false upgrade to Internet Explorer program makes several modifications to the system and attempts to contact other remote systems.

Within the Trojan horse util-linux distribution the program /bin/login was modified. The modifications included code to send email to an intruder that contains the host name and uid of users logging in. The code was also modified to provide anyone with access to a login prompt the capability of executing commands based on their input at the login prompt.

CA-99.03
FTP Buffer Overflows
To aid in the wide distribution of essential security information, the CERT Coordination Center forwarded information from Netect, Inc regarding a potential root compromise resulting from a remote buffer overflow on various FTP servers.

Due to insufficient bounds checking, it is possible to subvert an ftp server by corrupting its internal stack space. By supplying carefully designed commands to the ftp server, intruders can force the server to execute arbitrary commands with root privilege. Intruders who are able to exploit this vulnerability can ultimately gain interactive access to the remote ftp server with root privilege.

One temporary workaround against an anonymous attack is to disable any world writable directories the user may have access to by making them read only. This will prevent an attacker from building an unusually large path, which is required in order to execute these particular attacks. The permanent solution is to install a patch from your Vendor, or locate one provided by the Software's author or maintainer.

CA-99.04
Melissa Macro Virus
The Melissa macro virus propagates in the form of an email message containing an infected Word document as an attachment. When a user opens an infected .doc file with Microsoft Word97 or Word2000, the macro virus is immediately executed if macros are enabled.

Upon execution, the virus first lowers the macro security settings to permit all macros to run when documents are opened in the future. Therefore, the user will not be notified when the virus is executed in the future.

CA-99.05
Vulnerability in statd Exposes Vulnerability in automountd
There are two vulnerabilities, one in statd and one in automountd, that are being used together by intruders to gain access to vulnerable systems. By combining attacks exploiting these two vulnerabilities, a remote intruder is able to execute arbitrary commands with the privileges of the automountd service.

CA-99.06
ExploreZip Trojan Horse Program
The ExploreZip Trojan horse has been propagated between users in the form of email messages containing an attached file named zipped_files.exe. (Some email programs may display this attachment with a "WinZip" icon.) Users who execute the zipped_files.exe Trojan horse will infect the host system, potentially causing targeted files to be destroyed and may also infect other networked systems that have writable shares. Because of the large amount of network traffic generated by infected machines, network performance may suffer and indirectly, this Trojan horse could cause a denial of service on mail servers.

CA-99.07
IIS Buffer Overflow
There is a buffer overflow vulnerability in Microsoft Internet Information Server (IIS) 4.0. These vulnerabilities allow remote intruders to execute arbitrary code with the privileges of the IIS server. Additionally, intruders can use this vulnerability to crash vulnerable IIS processes.

A tool to exploit this vulnerability has been publicly released.

CA-99.08
Buffer Overflow Vulnerability in Calendar Manager Service Daemon, rpc.cmsd
A buffer overflow vulnerability has been discovered in the Calendar Manager Service daemon, rpc.cmsd. The rpc.cmsd daemon is frequently distributed with the Common Desktop Environment (CDE) and Open Windows. When exploited this vulnerability allows remote and local users to execute arbitrary code with the privileges of the rpc.cmsd daemon, typically root. (Under some configurations rpc.cmsd runs with an effective userid of daemon, while retaining root privileges.)

CA-99.09
Array Services Default Configuration
A vulnerability has been discovered in the default configuration of the Array Services daemon, arrayd. The default configuration of SGI Array Services disables authentication and allows remote and local users to execute arbitrary commands as root.

CA-99.10
Insecure Default Configuration on RaQ2 Servers
A vulnerability has been discovered in the default configuration of Cobalt Networks RaQ2 servers that allows remote users to install arbitrary software packages to the system. This access can then be used to gain root privileges on the system

CA-99.11
Vulnerabilities in the Common Desktop Environment
Multiple vulnerabilities have been identified in some distributions of the Common Desktop Environment (CDE). By exploiting these vulnerabilities:

- A local or remote user can run commands on a vulnerable system with the same privileges as that of the attacked ttsession.
- A local user can run arbitrary commands or execute arbitrary code as root.

CA-99.12
Buffer Overflow in amd
There is a buffer overflow vulnerability in the logging facility of the amd daemon. By exploiting this vulnerability, remote intruders can execute arbitrary code as the user running the amd daemon (usually root).

CA-99.13
Multiple Vulnerabilities in WU-FTPD
Vulnerabilities have been identified in WU-FTPD and other ftp daemons based on the WU-FTPD source code. By exploiting these vulnerabilities:

- Remote and local intruders are able to execute arbitrary code as the user running the ftpd daemon, usually root.
- Remote and local intruders who can connect to the FTP server can cause the server to consume excessive amounts of memory, preventing normal system operation.

CA-99.14
Multiple Vulnerabilities in BIND
Vulnerabilities have been found in BIND, the popular domain name server from the Internet Software Consortium (ISC). By exploiting these vulnerabilities:

- Remote intruders can execute arbitrary code with the privileges of the user running named, typically root.
- Remote intruders can disrupt the normal operation of your name server, possibly causing a crash.

- Remote intruders can disrupt the ability of your name server to respond to legitimate queries. By intermittently exercising this vulnerability, intruders can seriously degrade the performance of your name server.
- Local intruders can cause named to crash if they can gain write access to your zone files.

CA-99.15
Buffer Overflows in SSH daemon and RSAREF2 Library

Some versions of sshd are vulnerable to a buffer overflow that can allow an intruder to influence certain variables internal to the program. This vulnerability alone does not allow an intruder to execute code. However, a vulnerability in RSAREF2 can be used in conjunction to allow a remote intruder to execute arbitrary code.

CA-99.16
Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind

All versions of sadmind, part of Sun Microsystems' Solstice AdminSuite package, are vulnerable to a buffer overflow that can allow a remote user to execute arbitrary code with root privileges.

Appendix B: CERT Incident Notes Issued in 1999

The following incident notes were published in 1999. Incident Notes describe current intruder activities that have been reported to the CERT/CC incident response team. Incident Notes are available on the CERT Web site at http://www.cert.org/.

IN-99.01
"sscan" Scanning Tool
Intruders are using the sscan tool to perform probes against victim hosts to identify services that may potentially be vulnerable to exploitation. Though sscan itself does not attempt to exploit vulnerabilities, it can be configured to automatically execute scripts of commands that can be maliciously crafted to exploit vulnerabilities. Thus, it is possible for an unpredictable set of attacks to be mounted against a victim site in conjunction with the sscan probes.

IN-99.02
Happy 99 Trojan Horse
The first time Happy99.exe is executed, a fireworks display saying "Happy 99" appears on the computer screen and, at the same time, modifies system files. The executable affects Microsoft Windows 95/98 and NT machines by

- copying the WSOCK32.DLL file to WSOCK32.SKA
- modifying the WSOCK32.DLL file, which is used for Internet connectivity
- creating files called SKA.EXE and SKA.DLL in the system directory
- creating an entry in the registry to start SKA.EXE

Once Happy99 is installed, every email and Usenet posting sent by an affected user triggers Happy99 to send a follow up message containing Happy99.exe as a uuencoded attachment. Happy99 keeps track of who received the Trojan horse message in a file called LISTE.SKA in the system folder.

IN-99.03
CIH/Chernobyl Virus
The CIH virus, or the Chernobyl virus infects executable files and is spread by executing an infected file. Since many files are executed during normal use of a computer, the CIH virus can infect many files quickly.

There are several variants of the CIH virus. Some activate every month on the 26th, while other variants activate just on April 26th or June 26th. Once the CIH virus activates, the virus attempts to erase the entire hard drive and to overwrite the system BIOS. Some machines may require a new BIOS chip to recover if overwritten by the CIH virus. CIH only affects Win95/98 machines.

IN-99.04
Similar Attacks Using Various RPC Services
Reports indicate that intruders exploited three different RPC service vulnerabilities. The scope of the incidents suggests that intruders are using scripts to automate attacks. These attacks appear to attempt multiple exploitations but produce similar results. Vulnerabilities exploited as a part of these attacks include:

- CA-99-08 - Buffer Overflow Vulnerability in rpc.cmsd
- CA-99-05 - Vulnerability in statd exposes vulnerability in automountd
- CA-98.11 - Vulnerability in ToolTalk RPC Service

IN-99.05
Systems Compromised Through a Vulnerability in am-utils
Reports submitted indicate that intruders are actively exploiting a vulnerability in amd that is resulting in remote users gaining root access to victim machines. The vulnerability exploited as a part of these attacks is CA-99-12, Buffer Overflow in amd.

IN-99.06
Distributed Network Sniffer
Reports indicate that intruders are using distributed network sniffers to capture usernames and passwords. The distributed sniffer consists of a client and a server portion. The sniffer clients have been found exclusively on compromised Linux hosts.

IN-99.07
Distributed Denial of Service Tools
Reports indicate that intruders are installing distributed denial of service tools. These tools utilize distributed technology to create large networks of hosts capable of launching large coordinated packet flooding denial of service attacks.

IN-99.08
Attacks Against IIS Web Servers Involving MDAC
Reports indicate that IIS web servers were compromised via a vulnerability in MS Data Access Components (MDAC).

Appendix C: CERT Vulnerability Notes Issued in 1999

The following Vulnerability Notes were published in 1999. Vulnerability Notes describe weaknesses in Internet-related systems that could be exploited but that do not currently meet the criteria for advisories. Vulnerability Notes are available on the CERT Web site at http://www.cert.org/.

VN-99.01
Potential for False Authentication in Registry Transactions

Internet registries have the authority to delegate specific portions of domain name and/or IP address space to other entities. In the absence of secure transaction authentication, automated and manual registry transaction processes may be vulnerable to forged requests, leading to serious results.

VN-99.02
Microsoft Windows NT 4.0 Local Security Authority May Be Crashed by Malformed Messages

There is a vulnerability in Microsoft NT Local Security Authority (LSA) service may allow unauthorized agents to crash the service.

By sending the LSA service an improperly constructed message, an unauthenticated remote user may be able to overflow an unchecked buffer causing the LSA service and its subsystems to cease functioning.

VN-99.03
Vulnerability in the MBone Session Directory Manager Package SDR

There is a vulnerability in the MBone SDR package that allows certain metacharacters embedded in Session Initiation Protocol (SIP) messages the SDR receives to be interpreted and possibly executed with the same privileges as the process running the SDR package. Sites running versions of SDR 2.6.2 or older for Windows and Unix platforms are vulnerable.