Software Engineering Institute
Carnegie Mellon University

CERT® Coordination Center 2000 Annual Report

April 2001

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 comprehensive view of attack methods, vulnerabilities, and the impact of attacks on information systems and networks; provide information on incident and vulnerability trends and characteristics
- Build an infrastructure of increasingly competent security professionals who respond quickly to attacks on Internet-connected systems and are able to protect their systems against security compromises
- Provide methods to evaluate, improve, and maintain the security and survivability of networked systems
- Work with vendors to improve the security of as-shipped products

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 2000 were survivable network management practices, survivable network technology, security incident handling and analysis, vulnerability analysis, and information services.

We develop and publish security practices that provide concrete, practical guidance that helps organizations improve the security of their networked computer systems. These practices, published as security improvement modules, enable experienced administrators to protect systems and information against both malicious and inadvertent compromises.

We are currently conducting pilots of the Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE[SM]), a self-directed evaluation method for identifying and managing information security risks. OCTAVE 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 assets to the identified threats. By putting together these individual components, the enterprise can begin to understand what information is at risk. With this understanding, the enterprise can create a protection strategy that reduces the overall risk exposure of its information assets. The OCTAVE 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.

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 large 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 handling 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 trends and analyzing high-impact threats and vulnerabilities, such as

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

Our computer security incident handling 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 security problems and potential solutions comes from experience with compromised sites on the Internet and 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: majordomo@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 Handling

From January through December 2000, the CERT/CC received 56,365 email messages and more than 1,280 hotline calls reporting computer security incidents or requesting information. We received 774 vulnerability reports and handled 21,756 computer security incidents during this period. More than 9,350,000[1] hosts were affected by these incidents.

We continue to provide advice to computer system administrators in the Internet community who report security problems. In addition, one of our primary objectives is to understand the state of Internet security and convey that information to the system administrators, network managers, and others in the Internet community.

When we receive a vulnerability report, CERT/CC vulnerability experts analyze the potential vulnerability, working with technology producers, vendors, and Internet security experts. 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 2000.

1. **Distributed Denial of Service (DDoS)**
   The year began with extensive denial-of-service attacks using tools that take advantage of the distributed nature of the Internet. In addition to continued reports of denial-of-service problems, a denial-of-service tool called "stacheldraht" was discovered (CA-2000-01, which elaborated on and supplemented information released in an earlier denial-of-service advisory (CA-1999-17).). In April, we began receiving reports of intruders using nameservers to execute packet flooding denial-of-service attacks (IN-2000-04). The CERT/CC also learned of two serious denial-of-service vulnerabilities in the Internet Software Consortium's (ISC) BIND software (CA-2000-20).

[1] Host counts do not include estimated numbers of uncounted/unspecified hosts in all reported reconnaissance/probe/scanning incidents.

Distributed denial-of-service attacks were analyzed in a report released in late 1999. The report included recommendations for managers, system administrators, Internet service providers, and others.

2. **BIND**
   Intruders root compromised systems through vulnerabilities in BIND including the "NXT bug" described in advisory CA-1999-14. This activity had been ongoing since late last year. The CERT/CC published advice on protecting systems that run BIND nameservers in CA-1999-14 and CA-2000-03.

   In addition, two serious denial-of-service vulnerabilities were identified this year: the "zxfr bug" and the "srv bug." Though the CERT/CC has not yet received reports of these vulnerabilities being exploited, the potential is there. Advice has been published in CA-2000-20.

3. **FTP**
   Intruders exploited vulnerabilities in WU-FTPD and other FTP daemons to gain root access. They scanned large network blocks searching for vulnerable machines and used automated tools to compromise the ones they found. In some cases, the intruder tool included a denial-of-service tool, a password sniffer, and more.

   One target for scanning was a vulnerability in "site exec" or "ireply." This vulnerability is the result of missing character-formatting argument in several function calls. Normally if "site exec" is enabled, a user logged into an FTP server (including the "ftp" or "anonymous" user) may execute a restricted subset of quoted commands on the server itself. However, malicious users have been able to trick the FTP daemon into executing, as root, any code they choose. (CA-2000-13 and IN-2000-10)

4. **rcp.statd**
   Intruders used vulnerabilities in rpc.statd to gain root access and execute programs of their choice. This was possible because the rpc.statd program passes user-supplied data to another function (syslog) without validating it. One reason the attacks have been widespread is that insecure default configurations have been enabled during automated installation and upgrade processes. As with the FTP exploitations, intruders performed widespread scans for this vulnerability and used toolkits to automate their attacks on vulnerable machines. As a result, they were able to compromise hundreds of hosts in a single incident. (CA-2000-17 and IN-2000-10)

5. **ActiveX Controls**
   In 2000, we received reports of email-borne viruses that exploit a vulnerability in the Microsoft ActiveX control named "Scriptlet.Typelib." This ActiveX control allows local files to be created or modified, so it is unsafe to allow untrusted programs to access this control (IN-2000-06). Additionally, we published information about a serious vulnerability in the HHCtrl

ActiveX control. This vulnerability allows remote intruders to execute arbitrary code, if the intruder can cause a compiled help file (CHM) to be accessed locally (CA-2000-12).

To raise awareness in the Internet community about the risks in unsafe ActiveX controls, we invited twenty security experts to address security issues related to ActiveX. Together, we identified situations under which ActiveX and related technologies may be used safely. The CERT/CC summarized the results of this workshop in a report that is available on the CERT/CC web site. The report includes a list of all known vulnerabilities involving ActiveX controls as of the date of the workshop.

6. **"Love Letter"**
   "Love Letter" gained a great deal of attention this year. It is a malicious VBScript program that spreads in a variety of ways. In addition to damage caused by "Love Letter," some sites suffered considerable network degradation as a result of mail, file, and web traffic generated as a result of "Love Letter." The CERT/CC published details in CERT advisory CA-2000-04.

2.1.2 FedCIRC

The CERT/CC incident handling team provides operational support to FedCIRC, the Federal Computer Incident Response Center. FedCIRC provides incident response and other security-related services to Federal civilian agencies. The CERT/CC focuses on incident and vulnerability analysis. FedCIRC is managed by the General Services Administration (GSA).

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 understanding of current security problems and potential solutions comes from our 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 issues identified 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.

2.3 Publications

2.3.1 Advisories

The CERT/CC published 22 advisories in 2000. 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.

To keep advisories current, we update them as we receive new information. The complete listing of advisories issued during 2000 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. Four summaries were issued in 2000. 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 handling team. Vulnerability notes describe weaknesses in Internet-related systems that could be exploited but that currently do not meet the criteria for advisories. New tools, policies, and procedures enable us to publish vulnerability notes more frequently. They are available through the

Vulnerability Notes Database, which is located at www.kb.cert.org/vuls/. In 2000, we published 10 incident notes and 47 vulnerability notes.

2.3.4 Survivable Network Management Practices

CERT security practices are easy-to-implement guidance for experienced system administrators. The practices are technology-neutral, so they apply to many operating systems and platforms. Implementation details for specific technologies accompany many of the practices. Practices available on the CERT web site and in hard copy include the following:

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

2.3.5 Survivable Network Technology

Information on Survivable Network Technology activities is in the following research papers published in 2000. The complete list of papers is available on the CERT web site:

- *Survivability—A New Security Paradigm for Protecting Highly Distributed Mission Critical Systems*
- *Survivable Network Analysis Method*
- *The Survivability Imperative: Protecting Critical Systems*
- *A Research Agenda for Survivable Systems*
- *Life-Cycle Considerations for Survivable Systems*
- *Life-Cycle Models for Survivable Systems*

2.3.6 Other Security Information

The CERT/CC captures lessons learned from handling incidents and vulnerability reports 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.

Staff also testified before Congress on a variety of Internet security issues:

- Testimony to the U.S. Senate Judiciary Committee—"Internet Security Issues"
- Testimony to the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information—"Removing Roadblocks to Cyber Defense"

- Testimony to the Committee on Government Reform Subcommittee on Government Management, Information, and Technology—computer security
- Testimony to the Senate Armed Services Committee Subcommittee on Emerging Threats and Capabilities—cyber security
- Testimony to the Subcommittee on Crime of the House Committee on the Judiciary and the Subcommittee on Criminal Justice Oversight of the Senate Committee on the Judiciary—Internet denial-of-service attacks
- Testimony to the Joint Economic Committee, U.S. Congress—computer security and the U.S. economy

2.4 Media Exposure

The CERT/CC works with the news media to raise the awareness of a broad population to the risks they face on the Internet and steps they can take to protect themselves. Ultimately, this increased awareness 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 referred to in a variety of publications including *USA Today*, *The Wall Street Journal*, *The Seattle Times*, *The Toronto Star*, *CNET News* (an online publication), *Computerworld*, *PC World*, *Federal Computer News*, *Information Security*, *Infoworld*, *Time*, *Forbes*, *US News & World Report*, *Business Week*, *Reader's Digest*, and a number of other newspapers and magazines located around the country.

In addition, CERT/CC operations were covered on a number of online news sites including CNN.com, The New York Times Online, CNETNews.com, MacWeek.com, and ABCNews.com, as well as a number of news programs including CNN, ABC News 20/20, MSNBC, and CNBC.

The CERT/CC was also named "Best Security Idea or Practice" by *Secure Computing* magazine. In remarks at the awards ceremony, CERT/CC was referred to as "a beacon to the rest of the information security world," a compliment to both our staff and sponsors.

2.5 Training

The NSS Program currently offers nine training coures. Five courses derive from the work of the CERT Coordination Center, providing introductory and advanced traning for technical staff and the management of computer security incident response teams. Four courses are centered around broader Internet security issues and security practices. Its Information Security for System and Network Administrators is an intensive five-day course for technical staff. Other offerings are

geared toward educating policymakers, managers, and senior executive who are responsible for the security of information assets. Public courses are offered periodically and can be attended by anyone, with a reduced charge for government personnel. In addition, customer-site courses are offered to individual organizations (a reduced fee is charged to government organizations). Courses offered in 2000 included the following:

- *Concepts and Trends in Information Security*
- *Information Security for System and Network Administrators*
- *Managing Risks to Information Assets*
- *Executive Role in Information Security: Risk and Survivability*
- *Managing Computer Security Incident Response Teams (CSIRTs)*
- *Computer Security Incident Handling for Technical Staff (Introduction)*
- *Computer Security Incident Handling for Technical Staff (Advanced)*
- *Overview of Managing a CSIRT*
- *Creating a Computer Security Incident Response Team*

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 ActiveX Workshop

On August 22-23, 2000, the CERT/CC hosted a workshop in Pittsburgh, PA for 20 invited experts to address security issues related to ActiveX controls. The primary goal of the workshop was to identify the situations under which ActiveX and related technologies may be used safely and to produce a paper describing security concerns and configuration guidance.

That goal was achieved, and the resulting paper, Results of the Security in ActiveX Workshop, which is available on the CERT/CC web site, serves not only to dispel unwarranted myths about the safety of using ActiveX but also to furnish guidance to network administrators and others faced with security issues involving mobile code in general and ActiveX in particular. ActiveX and similar mobile codes provide enhanced usability. The level of enhancement is significant enough for corporate and government users that Internet security policies and procedures should reflect "risk management" rather than "risk avoidance."

Part 1 of the paper provides an overview of ActiveX, including security concerns and security features. Following this general information are, in Part 2, suggestions and good practices for specific groups in the Internet community:

- managers
- system administrators and security personnel

- developers of ActiveX controls and software that uses them
- users who administer their own computers; anyone who doesn't have a system administrator or security expert managing their system

2.6.2 Protecting the Internet Infrastructure

The CERT/CC assigns a higher priority to incidents and vulnerabilities that directly affect 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 such as core operating systems and related applications. We also look closely at the activity reported by major archive sites and other computer security incident response teams.

In addition to this incident handling work, CERT/CC staff attended and participated in a number of discussions centered around critical infrastructure protection. CERT/CC technical staff participates in meetings of the National Security Telecommunications Advisory Committee's Network Security Information Exchange (NSTAC NSIE) group, which works to reduce vulnerabilities in critical infrastructures. We have also been working with USC/ISI to develop a project to improve the integrity of the Domain Name System (DNS). This project involves notifying operators of DNS servers running vulnerable versions of DNS server software that they should apply appropriate security patches or upgrades.

2.6.3 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. It is essential to have multiple incident response organizations, each serving a particular user group. The CERT/CC staff regularly works with sites to help their teams expand their capabilities and provides guidance to newly forming teams. In addition, courses for teams and their managers are available, as listed in Section 2.5.

2.6.4 Forum of Incident Response and Security Teams (FIRST)

The CERT/CC is a founding member of the Forum of Incident Response and Security Teams (FIRST). CERT/CC regularly participates in FIRST activities, including the 2000 Conference. 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 85 teams belong to FIRST.

2.6.5 Vendor Relations

CERT/CC has continued to work closely with technology producers to inform them of security issues relating to their products and to facilitate and track their responses to these problems. Staff members have worked to influence the vendors to improve the basic default security within their products and to include security topics in their standard customer training courses. We interact with more than 100 vendors.

Vendors often provide information to the CERT/CC for inclusion in advisories and vulnerability notes.

2.6.6 External Events

CERT/CC staff members were invited to give presentations and participate in conferences, workshops, and meetings during 2000. 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)
- 9th Annual USENIX Security Symposium
- SEI Symposium
- 2000 Forum of Incident Response and Security Teams (FIRST) Conference
- Defense Information Assurance Program Conference
- IEEE Symposium on Security and Privacy
- 16th Annual Security Technology Symposium and Exhibition
- Institute of Internal Auditors (IIA) Critical Infrastructure Assurance Conference
- "Security for a New Century" Congressional Study Group
- INET 2000—the 10th Annual Internet Society Conference
- OSW 2000 Open Source Workshop
- Republican National Convention—Staff presented information about computer security issues surrounding wide area networks like the Internet.
- Telecommunications and Information Security Workshop
- Burton Group Annual Conference
- SpaceComm 2000 Conference
- DARPA-Intrusion Detection Systems Evaluation Rethink Workshop
- DMSO (Defense Modeling and the Simulation Office) Industry Days 2000
- NDIA (National Defense Industrial Association) Joint Aerospace Weapon Symposium
- NDIA 16th Annual Security Technology Symposium
- ICSN 2000 (International Conference on Dependable Systems and Networks)
- 38th meeting of the IFIP Working Group 10.4 (Dependable Computing and Fault Tolerance)
- 13th IEEE Computer Security Foundations Workshop

- International Institute of Business Technologies FY2001 5th Annual Government Technology Managers Conference—"Managing the Critical Infrastructure & Information Systems Assurance Government's E-Business Services"
- New Security Paradigms Workshop 2000
- Jane's Conference on Transnational Organized Crime
- ISAAC '00—The Software Risk Management Conference

Appendix A: CERT Advisories Published in 2000

The following advisories were published in 2000. We update the advisories as necessary. Advisories are available on the CERT web site at http://www.cert.org/advisories/.

CA-2000-01
Denial-of-Service Developments
In addition to continued reports of denial-of-service problems, a denial-of-service tool called "stacheldraht" has been discovered.

CA-2000-02
Malicious HTML Tags Embedded in Client Requests
A web site may inadvertently include malicious HTML tags or script in a dynamically generated page based on unvalidated input from untrustworthy sources.

CA-2000-03
Continuing Compromises of DNS Servers
There are continuing compromises of machines running the DNS software that is part of BIND (named). A significant number of delegated DNS servers in the in-addr.apra tree are running outdated versions of DNS software.

CA-2000-04
Love Letter Worm
The Love Letter Worm is a malicious VBScript program that spreads in a variety of ways. Users can be infected by various means, including email, Windows file sharing, IRC, USENET news, and possibly via web pages.

CA-2000-05
Netscape Navigator Improperly Validates SSL Sessions
A flaw has been discovered in the way some web browsers validate SSL sessions. By exploiting this vulnerability, intruders may be able to deceive people into disclosing sensitive information (e.g. credit card numbers and other sensitive data) intended for a legitimate web site.

CA-2000-06
Multiple Buffer Overflows in Kerberos Authenticated Services
There are several buffer overflow vulnerabilities in the Kerberos authentication software. The most severe vulnerability allows remote intruders to gain root privileges on systems running services using Kerberos authentication. If vulnerable services are enabled on the Key Distribution Center (KDC) system, the entire Kerberos domain may be compromised.

CA-2000-07
Microsoft 2000 UA ActiveX Control Incorrectly Marked "Safe for Scripting"
The Microsoft Office 2000 UA ActiveX control is incorrectly marked as "safe for scripting". This vulnerability may allow for an intruder to disable macro warnings in Office products and, subsequently, execute arbitrary code. This vulnerability may be exploited by viewing an HTML document via a web page, newsgroup posting, or email message.

CA-2000-08
Inconsistent Warning Messages in Netscape Navigator
A flaw exists in Netscape Navigator that could allow an attacker to masquerade as a legitimate web site if the attacker can compromise the validity of certain DNS information. Attackers can trick users into disclosing information intended for a legitimate web site if the user has previously accepted a certificate in which the name recorded in the certificate does not match the DNS name of the web site to which the user is connecting.

CA-2000-09
Flaw in PGP 5.0 Key Generation
Under certain circumstances, PGP 5.0 generates keys that are not sufficiently random, which may allow an attacher to predict keys and, hence, recover information encrypted with that key.

CA-2000-10
Inconsistent Warning Messages in Internet Explorer
Several flaws exist in Microsoft Internet Explorer that could allow an attacker to masquerade as a legitimate web site if the attacker can compromise the validity of certain DNS information. These problems are different from the problems reported in CERT advisories CA-2000-05 and CA-2000-08, but they have a similar impact.

CA-2000-11
MIT Kerberos Vulnerable to Denial-of-Service Attacks
There are several potential buffer overflow vulnerabilities in the Kerberos authentication software. The most severe vulnerability allows remote intruders to disrupt normal operations of the Key Distribution Center (KDC) if an attacker is able to send malformed requests to a realm's key server. The vulnerabilities discussed in this advisory are different than the ones discussed in advisory CA-2000-06.

CA-2000-12
HHCtrl ActiveX Control Allows Local Files to be Executed
The HHCtrl ActiveX control has a serious vulnerability that allows remote intruders to execute arbitrary code, if the intruder can cause a compiled help file (CHM) to be stored "locally."

CA-2000-13
Two Input Validation Problems in FTPD
A vulnerability involving an input validation error in the "site exec" command has recently been identified in the Washington University ftpd (wu-ftpd) software package. A similar but distinct vulnerability has also been identified that involves a missing format string in several setproctitle() calls. It affects a broader number of ftp daemons.

CA-2000-14
Microsoft Outlook and Outlook Express Cache Bypass Vulnerability
Microsoft recently released Microsoft Security Bulletin MS00-046, in which they announced a patch for the "Cache Bypass" vulnerability. By exploiting this vulnerability, an attacker can use an HTML-formatted message to read certain types of files on the victim's machine.

CA-2000-15
Netscape Allows Java Applets to Read Protected Resources
Netscape Communicator and Navigator ship with Java classes that allow an unsigned Java applet to access local and remote resources in violation of the security policies for applets.

CA-2000-16
Microsoft "IE Script"/Access/OBJECT Tag Vulnerability
Under certain conditions, Internet Explorer can open Microsoft Access database or project files containing malicious code and execute the code without giving a user prior warning. Access files that are referenced by OBJECT tags in HTML documents can allow attackers to execute arbitrary commands using Visual Basic for Applications or macros.

CA-2000-17
Input Validation Problem in rpc.statd
The CERT/CC has begun receiving reports of an input validation vulnerability in the rpc.statd program being exploited. This program is included, and often installed by default, in several popular Linux distributions.

CA-2000-18
PGP May Encrypt Data With Unauthorized ADKs
Additional Decryption Keys (ADKs) is a feature of PGP (Pretty Good Privacy) that allows authorized extra decryption keys to be added to a user's public key certificate. However, an implementation flaw in PGP allows unsigned ADKs which have been maliciously added to a certificate to be used for encryption.

CA-2000-19
Revocation of Sun Microsystems Browser Certificates
To aid in the wide distribution of essential security information, the CERT Coordi-

nation Center is forwarding the following information from Sun Microsystems. Users who accept these certificates into their browser may inadvertently run malicious code signed by the compromised certificates.

CA-2000-20
Multiple Denial-of-Service Problems in ISC BIND
The CERT Coordination Center has recently learned of two serious denial-of-service vulnerabilities in the Internet Software Consortium's (ISC) BIND software.

CA-2000-21
Denial-of-Service Vulnerabilities in TCP/IP Stacks
A variety of denial-of-service vulnerabilities has been explored and documented by BindView's RAZOR Security Team. These vulnerabilities allow attackers to consume limited resources on victim machines.

CA-2000-22
Input Validation Problems in LPRng
A popular replacement software package to the BSD lpd printing service called LPRng contains at least one software defect, known as a "format string vulnerability," which may allow remote users to execute arbitrary code on vulnerable systems.