Software Engineering Institute
Carnegie Mellon University

CERT® Coordination Center 2001 Annual Report

February 2002

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 2001 were survivable enterprise management, survivable network technology, security incident handling and analysis, vulnerability analysis, and information services.

In the area of survivable enterprise management, we develop and publish security practices that provide concrete, practical guidance that helps organizations improve the security of their networked computer systems. These practices enable experienced administrators to protect systems and information against both malicious and inadvertent compromises. The practices are published on the CERT/CC web site and compiled in the book *The CERT® Guide to System and Network Security Practices*, published by Addison-Wesley.

We continue work on the Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE℠), 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 its mission, 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. We have released the OCTAVE Method Implementation Guide, which contains a complete set of information, instructions, and worksheets needed to perform the OCTAVE Method, and the OCTAVE Criteria, which defines the requirements for a comprehensive, self-directed, information security risk evaluation.

The area of survivable network technology keeps pace with evolving information system technology, threats, and vulnerabilities. Focused on system survivability (the ability of a system to provide essential services in the presence of attacks, accidents, and failures) and critical infrastructure protection, work is aimed at developers and acquirers of systems as well as at system operators.

Developers and acquirers need to understand the importance of building security and survivability into systems, rather than trying to add it on once the systems are installed. The Survivable Systems Analysis method helps system architects and designers systematically assess the survivability properties of proposed systems, existing systems, and planned modifications to existing systems.

The Emergent Algorithm project is developing a powerful system modeling, simulation, and analysis tool (Easel) that enables developers and researchers to uncover interactions in complex systems. Easel can be used to determine the effects of specific cyber attacks, accidents, and failures (survival scenarios) on large-scale systems of systems before development. It allows "what if" scenarios and provides information that can be used for contingency planning.

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

The CERT/CC helps the Internet community deal with its immediate problems and analyzes the scope and nature of the problems. 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 2001, the CERT/CC received 118,907 email messages and more than 1,417 hotline calls reporting computer security incidents or requesting information. We received 2,437 vulnerability reports and handled 52,658 computer security incidents during this period.

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.

2.1.1 Intruder Activity

Below we describe some of the most serious intruder activities reported to the CERT/CC in 2001.

1. **Multiple Vulnerabilities in BIND**
   Intruders root compromised systems through vulnerabilities in the Internet Software Consortium's Berkeley Internet Name Domain (BIND) server. The CERT/CC published advice on protecting systems that run BIND in CA-2001-02.

   In March 2001, intruders continued to compromise systems using two of the vulnerabilities described in CA-2001-02. The CERT/CC published additional advice in IN-2001-03, identifying the attack profiles and toolkits used in such attacks.

2. **sadmind/IIS Worm**
   Intruders used a piece of self-propagating malicious code (referred to here as sadmind/IIS) to exploit vulnerabilities in Solaris systems and IIS servers, thereby compromising systems and defacing web pages. The sadmind/IIS worm exploits a vulnerability in Solaris systems and subsequently installs software to attack Microsoft IIS web servers. In addition, it includes a component to propagate itself automatically to other vulnerable Solaris systems (CA-2001-11).
3. **"Code Red" Worm**
   The "Code Red" worm received a great deal of attention this year. On June 19, 2001, the CERT/CC published CA-2001-13, describing a vulnerability in Indexing Services used by Microsoft IIS 4.0 and IIS 5.0. One month later, the CERT/CC began receiving a large number of reports of a worm commonly referred to as "Code Red," a self-propagating malicious code

that exploits IIS-enabled systems. The CERT/CC detailed the Code Red attack cycle, systems affected, and the system and network footprints in CA-2001-19 and CA-2001-23.

In early August, the CERT/CC received reports of new self-propagating malicious code exploiting the vulnerability described in CA-2001-13. The "Code Red II" worm causes system level compromise and leaves a backdoor on certain machines running Windows 2000 (IN-2001-09).

4. **W32/Sircam Malicious Code**
   On July 25, 2001, the CERT/CC received reports of a malicious code that spreads through email and potentially through unprotected network shares. Sircam has a direct impact on both the computer which was infected as well as those with which it communicates over email (CA-2001-22).
5. **W32/Nimda Worm**
   The CERT/CC received reports of malicious code known as the "W32/Nimda worm" or the "Concept Virus (CV) v.5." This worm propagates itself via several methods, including email, network shares, or through an infected web site. Nimda also spreads from client to web server by scanning for back doors left behind by the "Code Red II" and "sadmind/IIS" worms. On September 18, The CERT/CC issued an advisory on Nimda (CA-2001-26).

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.

2.3 Publications

2.3.1 Advisories

The CERT/CC published 37 advisories in 2001. 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 2001 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 2001. 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 2001, we published 15 incident notes and 326 vulnerability notes.

2.3.4 Survivable Enterprise Management

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. Practices available on the CERT web site 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 2001 and available on the CERT/CC web site:

- *Foundations for Survivable System Development: Service Traces, Intrusion Traces, and Evaluation Models*
- *Attack Modeling for Information Security and Survivability*
- *Architectural Refinement for the Design of Survivable Systems*
- *Can We Ever Build Survivable Systems from COTS Components?*

Staff also published the following papers in 2001:

- "What to Expect of Network Intelligence Analysis," Second SMC IEEE Information Assurance Workshop, West Point, NY, June 2001
- "Countering CyberWar" NATO Review, Winter 2001-2002
- "Managing Software Development for Survivable Systems," *Annals of Software Engineering*, Volume 11, 2001, pp. 45-78.
- "Can Industry and Academia Collaborate to Meet the Need for Software Engineers?" *Cutter IT Journal*, June 2001, Vol. 14, No. 6, pp.32-39
- "Toward Survivable COTS-Based Systems," *Cutter IT Journal*, February 2001, Vol. 14, No. 2, pp.4-11

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 Pennsylvania House Committee on Commerce and Economic Development, Subcommittee on Economic Development—"Internet Fraud"
- Testimony to the House of Representatives Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations—"Computer Security Issues that Affect Federal, State, and Local Governments and the Code Red Worm"
- Testimony to the House of Representatives Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations—"Information Technology—Essential But Vulnerable: How Prepared Are We for Attacks?"

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 *Inside Healthcare Computing*, *Internet World*, *American Banker*, *USA Today*, *The Wall Street Journal*, *The Toronto Star*, *Los Angeles Times*, *Computerworld*, *IAnewsletter*, *Washington Post*, *Security Management*, *Government Technology*, *Information Security*, *Infoworld*, *US News & World Report*, *Business Week*, and a number of other newspapers and magazines located around the country. Topics were also picked up by the Associated Press.

In addition, CERT/CC operations were covered on a number of online news sites including CNN.com, CNETNews.com, and ABCNews.com, as well as a number of news programs including CNN, BBC London, National Public Radio, and ABC News.

2.5 Training

The NSS Program offers nine training courses. Five courses derive from the work of the CERT Coordination Center, providing introductory and advanced training for technical staff and the management of computer security incident response teams. Four courses are centered around broader Internet security issues and security practices. Other offerings are geared toward educating policymakers, managers, and senior executives 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 2001 included the following:

- *Concepts and Trends in Information Security*
- *Information Security for Technical Staff*
- *Managing Risks to Information Assets*
- *Survivability: A New Executive Perspective*—this course is now only available by arrangement
- *Managing Computer Security Incident Response Teams (CSIRTs)*
- *Computer Security Incident Handling for Technical Staff (Introductory)*
- *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 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. For example, 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.

2.6.2 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.

2.6.3 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 conferences and technical colloquia.

A current list of FIRST members is available from http://www.first.org/team-info/. Currently, more than 110 teams belong to FIRST.

2.6.4 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.

2.6.5 External Events

CERT/CC staff members were invited to give presentations and participate in conferences, workshops, and meetings during 2001. This has been an excellent way to educate people about network information system security and incident response. Staff members participated in the following conferences and meetings during 2001:

- Annual Computer Security Applications Conference
- 14th Conference on Software Engineering Education & Training
- 2001 Forum of Incident Response and Security Teams (FIRST) Conference
- IEEE Symposium on Security and Privacy
- INET 2001—the 11th Annual Internet Society Conference
- International Association of Police Chiefs Conference (IACP 2001)
- International Conference on Dependable Systems and Networks
- International Symposium on Requirements Engineering
- The Internet Corporation for Assigned Names and Numbers (ICANN) Conference
- 52nd Internet Engineering Task Force (IETF) Meeting
- LISA 2001—15th Systems Administration Conference
- National Colloquium for Information Systems Security Education (NCISSE)
- Network Security Information Exchange (NSIE)
- North American Network Operators Group (NANOG)
- SANS Network Security 2001—the 7th Annual Conference on Securing Networks and Systems
- Trusted Computing Forum 2001
- 10th Annual USENIX Security Symposium

Appendix A: CERT Advisories Published in 2001

The following advisories were published in 2001. We update the advisories as necessary. Advisories are available on the CERT web site at http://www.cert.org/advisories/.

CA-2001-01
Interbase Server Contains Compiled-in Back Door Account
Interbase is an open source database package that had previously been distributed in a closed source fashion by Borland/Inprise. Both the open and closed source versions of the Interbase server contain a compiled-in back door account with a known password.

CA-2001-02
Multiple Vulnerabilities in BIND
Domain Name System (DNS) Servers running various versions of ISC BIND (including both 4.9.x prior to 4.9.8 and 8.2.x prior to 8.2.3; 9.x is not affected) and derivatives. Because the normal operation of most services on the Internet depends on the proper operation of DNS servers, other services could be impacted if these vulnerabilities are exploited.

CA-2001-03
VBS/OnTheFly (Anna Kournikova) Malicious Code
"VBS/OnTheFly" is a VBScript program that spreads via email. This malicious code can infect a system if the enclosed attachment is run.

CA-2001-04
Unauthentic "Microsoft corporation" Certificates
On January 29 and 30, 2001, VeriSign, Inc. issues two certificates to an individual fraudulently claiming to be an employee of Microsoft Corporation. Any code signed by these certificates will appear to be legitimately signed by Microsoft when, in fact, it is not. Once accepted, these certificates may allow an attacker to execute malicious code on the user's system.

CA-2001-05
Exploitation of snmpXdmid
The CERT/CC has received numerous reports indicating that a vulnerability in snmpXdmid is being actively exploited. Exploitation of this vulnerability allows an intruder to gain privileged (root) access to the system.

CA-2001-06
Automatic Execution of Embedded MIME Types
Microsoft Internet Explorer has a vulnerability triggered when parsing MIME parts in a document that allows a malicious agent to execute arbitrary code.

CA-2001-07
File Globbing Vulnerabilities in Various FTP Servers
Several File Transfer Protocol (FTP) servers incorrectly manage buffers in a way that can lead to remote intruders executing arbitrary code on the FTP server.

CA-2001-08
Multiple Vulnerabilities in Alcatel ADSL Modems
The San Diego Supercomputer Center (SDSC) has recently discovered several vulnerabilities in the Alcatel Speed Touch Asymmetric Digital Subscriber Line (ADSL) modem.

CA-2001-09
Statistical Weaknesses in TCP/IP Initial Sequence Numbers
A new vulnerability has been identified which is present when using random increments to constantly increase TCP ISN values over time. Systems are vulnerable if they have not incorporated RFC1948 or equivalent improvements or do not use cryptographically secure network protocols like IPsec.

CA-2001-10
Buffer Overflow Vulnerability in Microsoft IIS 5.0
A vulnerability exists in Microsoft IIS 5.0 running on Windows 2000 that allows a remote intruder to run arbitrary code on the victim machine, allowing them to gain complete administrative control of the machine.

CA-2001-11
sadmind/IIS Worm
The CERT/CC has received reports of a new piece of self-propagating malicious code (also called the sadmind/IIS worm). The worm uses two well-known vulnerabilities to compromise systems and deface web pages.

CA-2001-12
Superfluous Decoding Vulnerability in IIS
A serious vulnerability in Microsoft IIS may allow remote intruders to execute commands on an IIS web server. This vulnerability closely resembles a previous vulnerability in IIS that was widely exploited.

CA-2001-13
Buffer Overflow In IIS Indexing Service DLL
A vulnerability exists in the Indexing Services used by Microsoft IIS 4.0 and IIS 5.0 running on Windows NT, Windows 2000, and beta versions of Windows XP. This vulnerability allows a remote intruder to run arbitrary code on the victim machine.

CA-2001-14
Cisco IOS HTTP Server Authentication Vulnerability
A problem with HTTP server component of Cisco IOS system software allows an

intruder to execute privileged commands on Cisco routers if local authentication databases are used.

CA-2001-15
Buffer Overflow in Sun Solaris in.lpd Print Daemon
A buffer overflow exists in the Solaris BSD-style line printer daemon, in.lpd, that may allow a remote intruder to execute arbitrary code with the privileges of the running daemon.

CA-2001-16
Oracle 8i contains buffer overflow in TNS listener
A vulnerability in Oracle 8i allows remote intruders to assume control of database servers running on victim machines. If the Oracle server is running on a Windows system, an intruder may also be able to gain control of the underlying operating system.

CA-2001-17
Check Point RDP Bypass Vulnerability
A vulnerability in Check Point FireWall-1 and VPN-1 may allow an intruder to pass traffic through the firewall on port 259/UDP.

CA-2001-18
Multiple Vulnerabilities in Several Implementations of the Lightweight Directory Access Protocol (LDAP)
Several implementations of the Lightweight Directory Access Protocol (LDAP) contain vulnerabilities that may allow denial-of-service attacks, unauthorized privileged access, or both.

CA-2001-19
"Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service
The CERT/CC has received reports of new self-propagating malicious code that exploits certain configurations of Microsoft Windows susceptible to the vulnerability described in CERT advisory CA-2001-13 Buffer Overflow In IIS Indexing Service DLL. These reports indicate that the "Code Red" worm may have already affected as many as 225,000 hosts, and continues to spread rapidly.

CA-2001-20
Continuing Threats to Home Users
This year, we have seen a significant increase in activity resulting in compromises of home user machines. In many cases, these machines are then used by intruders to launch attacks against other organizations. Home users have generally been the least prepared to defend against attacks. Many home users do not keep their machines up to date with security patches and workarounds, do not run current anti-virus software, and do not exercise caution when handling email attachments. Intruders know this, and we have seen a marked increase in intruders specifically targeting home users who have cable modem and DSL connections.

CA-2001-21
Buffer Overflow in telnetd
The telnetd program is a server for the Telnet remote virtual terminal protocol. There is a remotely exploitable buffer overflow in Telnet daemons derived from BSD source code. This vulnerability can crash the server or be leveraged to gain root access.

CA-2001-22
W32/Sircam Malicious Code
"W32/Sircam" is malicious code that spreads through email and potentially through unprotected network shares. Once the malicious code has been executed on a system, it may reveal or delete sensitive information.

CA-2001-23
Continued Threat of the "Code Red" Worm
Since around July 13, 2001, at least two variants of the self-propagating malicious code "Code Red" have been attacking hosts on the Internet (see CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL. Different organizations who have analyzed "Code Red" have reached different conclusions about the behavior of infected machines when their system clocks roll over to the next month.

CA-2001-24
Vulnerability in OpenView and NetView
ovactiond is a component of OpenView by Hewlett-Packard Company and NetView by Tivoli, an IBM Company. These products are used to manage large systems and networks. There is a serious vulnerability in ovactiond that allows intruders to execute arbitrary commands with elevated privileges. This may subsequently lead to an intruder gaining administrative control of a vulnerable machine.

CA-2001-25
Buffer Overflow in Gauntlet Firewall allows intruders to execute arbitrary code
A vulnerability for a remotely exploitable buffer overflow exists in Gauntlet Firewall by PGP Security.

CA-2001-26
Nimda Worm
The CERT/CC has received reports of new malicious code known as the "W32/Nimda worm" or the "Concept Virus (CV) v.5." This new worm appears to spread by multiple mechanisms.

CA-2001-27
Format String Vulnerability in CDE ToolTalk
There is a remotely exploitable format string vulnerability in the CDE ToolTalk

RPC database service. This vulnerability could be used to crash the service or execute arbitrary code, potentially allowing an intruder to gain root access.

CA-2001-28
Automatic Execution of Macros
An intruder can include a specially crafted macro in a Microsoft Excel or PowerPoint document that can avoid detection and run automatically regardless of the security settings specified by the user.

CA-2001-29
Oracle9iAS Web Cache vulnerable to buffer overflow
A remotely exploitable buffer overflow in the Oracle9iAS Web Cache allows intruders to execute arbitrary code or disrupt the normal operation of Web Cache.

CA-2001-30
Multiple Vulnerabilities in lpd
There are multiple vulnerabilities in several implementations of the line printer daemon (lpd). The line printer daemon enables various clients to share printers over a network.

CA-2001-31
Buffer Overflow in CDE Subprocess Control Service
There is a remotely exploitable buffer overflow vulnerability in a library function used by the CDE Subprocess Control Service. This vulnerability could be used to crash the service or to execute arbitrary code with root privileges.

CA-2001-32
HP-UX Line Printer Daemon Vulnerable to Directory Traversal
The HP-UX line printer daemon (rlpdaemon) enables various clients to share printers over a network. A remotely exploitable buffer overflow vulnerability exists in the rlpdaemon.

CA-2001-33
Multiple Vulnerabilities in WU-FTPD
WU-FTPD is a widely deployed software package used to provide File Transport Protocol (FTP) services on UNIX and Linux systems. There are two vulnerabilities in WU-FTPD that expose a system to potential remote root compromise by anyone with access to the FTP service.

CA-2001-34
Buffer Overflow in System V Derived Login
Several applications use login for authentication to the system. A remotely exploitable buffer overflow exists in login derived from System V. Attackers can exploit this vulnerability to gain root access to the server.

CA-2001-35
Recent Activity Against Secure Shell Daemons

There are multiple vulnerabilities in several implementations of the Secure Shell (SSH) protocol. The SSH protocol enables a secure communications channel from a client to a server. We are seeing a high amount of scanning for SSH daemons, and we are receiving reports of exploitation.

CA-2001-36
Microsoft Internet Explorer Does Not Respect Content-Disposition and Content-Type MIME Headers
Microsoft Internet Explorer contains a vulnerability in its handling of certain MIME headers in web pages and HTML email messages. This vulnerability may allow an attacker to execute arbitrary code on the victim's system when the victim visits a web page or views an HTML email message.

CA-2001-37
Buffer Overflow in UPnP Service on Microsoft Windows
Vulnerabilities in software included by default on Microsoft Windows XP, and optionally on Windows ME and Windows 98, may allow an intruder to execute arbitrary code on vulnerable systems, to launch denial-of-service attacks against vulnerable systems, or to use vulnerable systems to launch denial-of-service attacks against third-party systems.