Software Engineering Institute
Carnegie Mellon University

CERT® Coordination Center
2002 Annual Report

February 2003

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 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 2002 were survivable enterprise management, survivable network technology, security incident and vulnerability handling and analysis, information services, and training.

In the area of survivable enterprise management, we continue work on 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 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. The book *Managing Information Security Risks: The OCTAVE^{SM} Approach*, published by Addison-Wesley, expands upon the OCTAVE approach and method and begins looking at the broader issue of managing information security risks using OCTAVE as a foundation. In 2002, OCTAVE-S, a version of OCTAVE tailored for small organizations, was piloted.

In our effort to develop an OCTAVE community, we held the first OCTAVE Users' Forum on September 19-20, 2002. The forum featured a variety of presentations and offered users a chance to share their experiences.

To help users implement their risk management plan, we also publish security practices that provide concrete, practical guidance that helps organizations improve the security of their networked computer systems. These practices, which are published on the CERT/CC web site and compiled in the book *The CERT® Guide to System and Network Security Practices*, enable experienced administrators to protect systems and information against both malicious and inadvertent compromises. We recently published a new set of practices on outsourcing managed security services.

The area of survivable network technology concentrates on the technical basis for ensuring that a system can provide essential services in the presence of attacks, accidents, and failures, including critical infrastructure protection. 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 (SSA) method helps system architects and designers systematically assess the survivability properties of proposed systems, existing systems, and planned modifications to existing systems.

Easel, a powerful system modeling and simulation tool, enables system developers and owners to uncover interactions in complex systems. Easel can be used to identify previously undiscovered liabilities, plan protection strategies for interconnecting systems, and work to prevent unforeseen cascading effects upon linked infrastructures and systems.

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, or 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/

To enable managers and technical personnel to build their knowledge and skills, we offer courses in areas such as improving network security, creating and managing computer security incident response teams, and responding to and analyzing computer security incidents.

2 Highlights of CERT/CC Activities and Services

2.1 Incident Handling

From January through December 2002, the CERT/CC received 204,841 email messages and more than 880 hotline calls reporting computer security incidents or requesting information. We received 4,129 vulnerability reports and handled 82,094 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 two of the most serious intruder activities reported to the CERT/CC in 2002.

- **Exploitation of Vulnerabilities in Microsoft SQL Server**
  Intruders compromised systems through the automated exploitation of null or weak default sa passwords in Microsoft SQL Server and Microsoft Data Engine. The CERT/CC published advice on protecting systems that run Microsoft SQL Server in CA-2002-04.

  In July 2002, intruders continued to compromise systems and obtain sensitive information by exploiting several serious vulnerabilities in the Microsoft SQL Server. The CERT/CC published additional advice in CA-2002-22.

- **Apache/mod_ssl Worm**
  Intruders used a piece of self-propagating malicious code (referred to here as Apache/mod_ssl) to exploit a vulnerability in OpenSSL, an open-source implementation of the Secure Sockets Layer (SSL) protocol.

  The CERT/CC initially published CA-2002-23, describing four vulnerabilities in OpenSSL that could be used to create denial of service. When these and other vulnerabilities finally manifested themselves in the form of the Apache/mod_ssl Worm, the CERT/CC published advice in CA-2002-27.

2.1.2 Significant Vulnerabilities

Among the significant vulnerabilities this year are the two listed below, which affect the products of many different vendors.

- **Multiple Vulnerabilities in Bind**
  BIND received a great deal of attention this year. On November 14, 2002, the CERT/CC published CA-2002-31, describing multiple vulnerabilities in BIND, the popular domain name server and client library software package from the Internet Software Consortium (ISC). Some of these vulnerabilities may allow a remote intruder to execute arbitrary code with privileges of the user running named (typically root).
- **Multiple Vulnerabilities in SNMP**
  In February, the CERT/CC began receiving reports of vulnerabilities in multiple vendors' implementations of SNMP, the Simple Network Management Protocol. The CERT/CC documented these vulnerabilities in CA-2002-03, which highlighted related vulnerability notes, fixes, and affected vendors.

  Since the SNMP vulnerabilities had the potential to affect a large base of computers, the CERT/CC published an FAQ that focused on the details of SNMP.

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 2002. 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 2002 can be found in Appendix A.

2.3.2 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. They are available through the Vulnerability Notes Database, which is located at www.kb.cert.org/vuls/. In 2002, we published 6 incident notes and 375 vulnerability notes.

2.3.3 CERT Security 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. Practices available on the CERT web site include the following:

- *Outsourcing Managed Security Services*
- *Securing Desktop Workstations*
- *Responding to Intrusions*
- *Securing Network Servers*
- *Deploying Firewalls*
- *Securing Public Web Servers*
- *Detecting Signs of Intrusion*

2.3.4 Survivable Network Technology

Staff published numerous research papers in 2002 that deal with survivable network technology activities. The following samples are available on the CERT/CC web site:

- *Lifecycle Models for Survivable Systems*
- *Trustworthy Refinement Through Intrusion-Aware Design*
- *Flow-Service-Quality (FSQ) Engineering: Foundations for Network System Analysis and Development*

Some additional papers published in 2002 include

- "Models of Information Security Trend Analysis," SPIE Aerosense Law Enforcement Technologies Conference, Orlando, FL, April 2002
- "An Empirical Investigation of Six Software Error Detection Methods," *International Journal of Software Testing, Verification and Reliability*, Volume 12, May 2002, pp. 155-171
- "Foundations for Survivable Systems Engineering," *CrossTalk*, Volume 15, July 2002, pp. 10-15
- "Requirements Engineering and Technology Transfer: Obstacles, Incentives and Improvement Agenda," *Requirements Engineering Journal*, Volume 7, No. 3 (2002), pp.113-123
- "Can We Ever Build Survivable Systems from COTS Components," 14th International Conference, CAiSE '02, Toronto, Canada, May 2002, pp. 216-229
- "Assessing the Risk of COTS Usage in Survivable Systems," *Cutter IT Journal*, May 2002, Volume 15, No. 5, pp.15-21

2.3.5 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 House of Representatives Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations—"Information Technology—Essential But Vulnerable: Internet Security Trends"

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 *New York Stock Exchange Magazine*, *Federal Computer Week*, *Computerworld*, the *Washington Post*, *Scientific American*, the *Dow Jones News Service*, the *LA Times*, the *Chronicle of Higher Education*, *Forbes Magazine*, *Information Security*, *IEEE Software*, *Network World Magazine*, *USA Today*, the *Boston Herald*, *PC World*, *Security Management Magazine*, *Smart Computing*, *E-Commerce Times*, *Financial Times (UK)*, and a number of other newspapers and magazines located around the world. Topics were also picked up by the Associated Press.

In addition, CERT/CC operations were covered on a number of news programs and online news sites including CNN, ABC News, MSNBC, CBS News, National Public Radio, Internet.com, CNET News, BBC, and Frontline Public Television.

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. All courses can be licensed, and train-the-trainer sessions are available for all courses.

Courses offered in 2002 included the following:

- *Concepts and Trends in Information Security*
- *Information Security for Technical Staff*
- *OCTAVE^{SM} Method Training Workshop*
- *Information Survivability: A New Executive Perspective*
- *Creating a Computer Security Incident Response Team*
- *Overview of Managing a Computer Security Incident Response Team*
- *Managing Computer Security Incident Response Teams*
- *Fundamentals of Incident Handling*
- *Advanced Incident Handling for Technical Staff*

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 125 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 425 hardware and software developers.

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 2002. 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 2002:

- Conference on Software Engineering Education & Training
- Forum of Incident Response and Security Teams (FIRST) Conference
- IEEE Symposium on Security and Privacy
- International Information Integrity Institute (I4) Forum
- Network and Distributed System Security Symposium (NDSS)
- International Conference on Dependable Systems and Networks
- Information Survivability Workshop
- International Conference on COTS-Based Software Systems
- Internet Engineering Task Force (IETF) Meeting
- LISA 2002—16th Systems Administration Conference
- International Conference on Software Engineering (ICSE 2002)
- Network Security Information Exchange (NSIE)
- North American Network Operators Group (NANOG)
- New Security Paradigms Workshop 2002
- 6th Annual Information Assurance Workshop
- USENIX Security Symposium

Appendix A: CERT Advisories Published in 2002

The following advisories were published in 2002. We update the advisories as necessary. Advisories are available on the CERT web site at http://www.cert.org/advisories/.

CA-2002-01
Exploitation of Vulnerability in CDE Subprocess Control Service
The CERT/CC has received credible reports of scanning and exploitation of Solaris systems running the CDE Subprocess Control Service buffer overflow vulnerability identified in CA-2001-31 and discussed in VU#172583.

CA-2002-02
Buffer Overflow in AOL ICQ
There is a remotely exploitable buffer overflow in ICQ. Attackers that are able to exploit the vulnerability may be able to execute arbitrary code with the privileges of the victim user. Full details are discussed in VU#570167. An exploit is known to exist, but we do not believe it has been distributed in the wild. We have not seen active scanning for this vulnerability, nor have we received any reports of this vulnerability being exploited.

CA-2002-03
Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)
Numerous vulnerabilities have been reported in multiple vendor SNMP implementations. These vulnerabilities may allow unauthorized privileged access, denial-of-service attacks, or unstable behavior. If your site uses SNMP in any capacity, the CERT/CC encourages you to read this advisory and follow the advice provided in the solution section.

CA-2002-04
Buffer Overflow in Microsoft Internet Explorer
Microsoft Internet Explorer contains a buffer overflow vulnerability in its handling of embedded objects in HTML documents. This vulnerability could 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-2002-05
Multiple Vulnerabilities in PHP fileupload
Multiple vulnerabilities exist in the PHP scripting language. These vulnerabilities could allow a remote attacker to execute arbitrary code with the privileges of the PHP process.

CA-2002-06
Vulnerabilities in Various Implementations of the RADIUS Protocol
Remote Authentication Dial In User Service (RADIUS) servers are used for authentication, authorization and accounting for terminals that speak the RADIUS protocol. Multiple vulnerabilities have been discovered in several implementations of the RADIUS protocol.

CA-2002-07
Double Free Bug in zlib Compression Library
There is a bug in the zlib compression library that may manifest itself as a vulnerability in programs that are linked with zlib. This may allow an attacker to conduct a denial-of-service attack, gather information, or execute arbitrary code.

CA-2002-08
Multiple Vulnerabilities in Oracle Servers
Multiple vulnerabilities in Oracle Application Server have recently been discovered. These vulnerabilities include buffer overflows, insecure default settings, failures to enforce access controls, and failure to validate input. The impacts of these vulnerabilities include the execution of arbitrary commands or code, denial of service, and unauthorized access to sensitive information.

CA-2002-09
Multiple Vulnerabilities in Microsoft IIS
A variety of vulnerabilities exist in various versions of Microsoft IIS. Some of these vulnerabilities may allow an intruder to execute arbitrary code on vulnerable systems.

CA-2002-10

Format String Vulnerability in rpc.rwalld

The rwall daemon (rpc.rwalld) is a utility that is used to listen for wall requests on the network. When a request is received, it calls wall, which sends the message to all terminals of a time-sharing system. A format string vulnerability may permit an intruder to execute code with the privileges of the rwall daemon.

CA-2002-11

Heap Overflow in Cachefs Daemon (cachefsd)

Sun's NFS/RPC file system cachefs daemon (cachefsd) is shipped and installed by default with Sun Solaris 2.5.1, 2.6, 7, and 8 (SPARC and Intel architectures). A remotely exploitable vulnerability exists in cachefsd that could permit a remote attacker to execute arbitrary code with the privileges of the cachefsd, typically root.

CA-2002-12

Format String Vulnerability in ISC DHCPD

The Internet Software Consortium (ISC) provides a Dynamic Host Configuration Protocol Daemon (DHCPD), which is a server that is used to allocate network addresses and assign configuration parameters to hosts. A format string vulnerability may permit a remote attacker to execute code with the privileges of the DHCPD (typically root).

CA-2002-13

Buffer Overflow in Microsoft's MSN Chat ActiveX Control

Microsoft's MSN Chat is an ActiveX control for Microsoft Messenger, an instant messaging client. A buffer overflow exists in the ActiveX control that may permit a remote attacker to execute arbitrary code on the system with the privileges of the current user.

CA-2002-14

Buffer Overflow in Macromedia JRun

A remotely exploitable buffer overflow exists in Macromedia's JRun 3.0 and 3.1.

CA-2002-15

Denial-of-Service Vulnerability in ISC BIND 9

A denial-of-service vulnerability exists in version 9 of the Internet Software Consortium's (ISC) Berkeley Internet Name Domain (BIND) server. ISC BIND versions 8 and 4 are not affected. Exploiting this vulnerability will cause the BIND server to shut down.

CA-2002-16

Multiple Vulnerabilities in Yahoo! Messenger

There are multiple vulnerabilities in Yahoo! Messenger. Attackers that are able to exploit these vulnerabilities may be able to execute arbitrary code with the privileges of the victim user.

CA-2002-17

Apache Web Server Chunk Handling Vulnerability

There is a remotely exploitable vulnerability in the handling of large chunks of data in web servers that are based on Apache source code. This vulnerability is present by default in configurations of Apache web servers versions 1.3 through 1.3.24 and versions 2.0 through 2.0.36. The impact of this vulnerability is dependent upon the software version and the hardware platform the server is running on.

CA-2002-18

OpenSSH Vulnerabilities in Challenge Response Handling

There are two related vulnerabilities in the challenge response handling code in OpenSSH versions 2.3.1p1 through 3.3. They may allow a remote intruder to execute arbitrary code as the user running sshd (often root). The first vulnerability affects OpenSSH versions 2.9.9 through 3.3 that have the challenge response option enabled and use SKEY or BSD_AUTH authentication. The second vulnerability affects PAM modules using interactive keyboard authentication in OpenSSH versions 2.3.1p1 through 3.3, regardless of the challenge response option setting.

CA-2002-19

Buffer Overflows in Multiple DNS Resolver Libraries

Buffer overflow vulnerabilities exist in multiple implementations of DNS resolver libraries. Operating systems and applications that utilize vulnerable DNS resolver libraries may be affected.

CA-2002-20

Multiple Vulnerabilities in CDE ToolTalk

Two vulnerabilities have been discovered in the Common Desktop Environment (CDE) ToolTalk RPC database server. The first vulnerability could be used by a remote attacker to delete arbitrary files, cause a denial of service, or possibly execute arbitrary code or commands. The second vulnerability could allow a local attacker to overwrite arbitrary files with contents of the attacker's choice.

CA-2002-21

Vulnerability in PHP

A vulnerability has been discovered in PHP. This vulnerability could be used by a remote attacker to execute arbitrary code or crash PHP and/or the web server.

CA-2002-22

Multiple Vulnerabilities in Microsoft SQL Server

The Microsoft SQL Server contains several serious vulnerabilities that allow remote attackers to obtain sensitive information, alter database contents, compromise SQL servers, and, in some configurations, compromise server hosts.

CA-2002-23

Multiple Vulnerabilities in OpenSSL

There are four remotely exploitable buffer overflows in OpenSSL. There are also encoding problems in the ASN.1 library used by OpenSSL. Several of these vulnerabilities could be used by a remote attacker to execute arbitrary code on the target system. All could be used to create denial of service.

CA-2002-24

Trojan Horse OpenSSH Distribution

The CERT/CC has received confirmation that some copies of the source code for the OpenSSH package were modified by an intruder and contain a Trojan horse. We strongly encourage sites which employ, redistribute, or mirror the OpenSSH package to immediately verify the integrity of their distribution.

CA-2002-25

Integer Overflow In XDR Library

There is an integer overflow present in the xdr_array() function distributed as part of the Sun Microsystems XDR library. This overflow has been shown to lead to remotely exploitable buffer overflows in multiple applications, leading to the execution of arbitrary code. Although the library was originally distributed by Sun Microsystems, multiple vendors have included the vulnerable code in their own implementations.

CA-2002-26

Buffer Overflow in CDE ToolTalk

The Common Desktop Environment (CDE) ToolTalk RPC database server contains a buffer overflow vulnerability that could allow a remote attacker to execute arbitrary code or cause a denial of service.

CA-2002-27

Apache/mod_ssl Worm

The CERT/CC has received reports of self-propagating malicious code which exploits a vulnerability (VU#102795) in OpenSSL. This malicious code has been referred to as Apache/mod_ssl worm, linux.slapper.worm and bugtraq.c worm.

CA-2002-28

Trojan Horse Sendmail Distribution

The CERT/CC has received confirmation that some copies of the source code for the Sendmail package were modified by an intruder to contain a Trojan horse. Sites that employ, redistribute, or mirror the Sendmail package should immediately verify the integrity of their distribution.

CA-2002-29

Buffer Overflow in Kerberos Administration Daemon

Multiple Kerberos distributions contain a remotely exploitable buffer overflow in the Kerberos administration daemon. A remote attacker could exploit this vulnerability to gain root privileges on a vulnerable system.

CA-2002-30

Trojan Horse tcpdump and libpcap Distributions

The CERT/CC has received reports that several of the released source code distributions of the libpcap and tcpdump packages were modified by an intruder and contain a Trojan horse. We strongly encourage sites that use, redistribute, or mirror the libpcap or tcpdump packages to immediately verify the integrity of their distribution.

CA-2002-31

Multiple Vulnerabilities in BIND

Multiple vulnerabilities with varying impacts have been found in BIND, the popular domain name server and client library software package from the Internet Software Consortium (ISC).

CA-2002-32

Backdoor in Alcatel OmniSwitch AOS

Alcatel has recently discovered a serious vulnerability in AOS version 5.1.1. Exploitation of this vulnerability can lead to full administrative control of the device running AOS.

CA-2002-33

Heap Overflow Vulnerability in Microsoft Data Access Components (MDAC)

A vulnerability in the Microsoft Data Access Components (MDAC) could lead to remote execution of code with the privileges of the current process or user.

CA-2002-34

Buffer Overflow in Solaris X Window Font Service

The Solaris X Window Font Service (XFS) daemon (fs.auto) contains a remotely exploitable buffer overflow vulnerability that could allow an attacker to execute arbitrary code or cause a denial of service.

CA-2002-35

Vulnerability in RaQ Server Appliances

A remotely exploitable vulnerability has been discovered in Sun Cobalt RaQ 4 Server Appliances running Sun's Security Hardening Package (SHP). Exploitation of this vulnerability may allow remote attackers to execute arbitrary code with superuser privileges.

CA-2002-36

Multiple Vulnerabilities in SSH Implementations

Multiple vendors' implementations of the secure shell (SSH) transport layer protocol contain vulnerabilities that could allow a remote attacker to execute arbitrary code with the privileges of the SSH process or cause a denial of service. The vulnerabilities affect SSH clients and servers, and they occur before user authentication takes place.

CA-2002-37

Buffer Overflow in Microsoft Windows Shell

A buffer overflow vulnerability exists in the Microsoft Windows Shell. An attacker can exploit this vulnerability by enticing a victim to read a malicious email message, visit a malicious web page, or browse to a folder containing a malicious .MP3 or .WMA file. The attacker can then execute arbitrary code with the privileges of the victim.