Software Engineering Institute
Carnegie Mellon University

CERT/CC 2003 Annual Report

CERT Division

http://www.sei.cmu.edu

REV-03.18.2016.0

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. The program's main areas of activity for 2003 included survivable enterprise management, analysis, security incident and vulnerability handling and analysis, and training.

Survivable Enterprise Management
Since it became freely available in June 2003, 2,600 people have downloaded the Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE℠) Method, bringing the total number of downloads since its development to 4,400. OCTAVE-S, a version of OCTAVE tailored for small organizations, is now also available from the CERT/CC web site and has been downloaded by more than 2,800 people from 80 countries.

We have also made progress with our work on the e-Authentication Risk and Requirements Assessment approach. In 2003, 24 federal e-Government initiatives used it to determine the authentication requirements of their electronic government transactions.

Analysis
Our staff has codified the Critical Systems Protection Initiative methodology for use by United States Secret Service (USSS) field agents in support of National Special Security Events. The USSS Critical Systems Protection Initiative is a collaborative effort to augment USSS protective measures.

The network situational awareness team has placed innovative tools and training materials in the open source community. The System for Internet Level Knowledge (SiLK) is a collection of tools that facilitates security analysis of netflow data collected from large networks. It consists of two

sets of tools-a packing system and an analysis suite-that collect and examine netflow data, allowing analysts to rapidly query large sets of data. Documentation accompanies the tool sets.

Incident and Vulnerability Handling and Analysis
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/

Training
To enable managers and technical personnel to build their knowledge and skills, we offer training in areas such as improving network security, creating and managing computer security incident response teams, and responding to and analyzing computer security incidents. In 2003, staff developed and implemented a new certification for incident handlers: the CERT®-Certified Computer Security Incident Handler program. The program requires that individuals meet training and experience requirements and pass an examination to be certified. As part of our work with incident response teams, we published *Handbook of Computer Security Incident Response Teams, 2nd edition* and *State of the Practice of Computer Security Incident Response Teams* in 2003.

--Back to top.--

2 Highlights of CERT/CC Activities and Services

2.1. Incident and Vulnerability Handling

From January through December 2003, the CERT/CC received 542,754 email messages and more than 934 hotline calls reporting computer security incidents or requesting information. We received 3,784 vulnerability reports and handled 137,529 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.

Intruder Activity

The following are two of the most serious intruder activities reported to the CERT/CC in 2003:

- **W32/Sobig.F Worm**
  The email-borne malicious program known as W32/Sobig.F relied on users to execute the email attachment manually or by using an email client that opened the attachment automatically. Once executed, the worm could download and execute code and send itself to email addresses it found on the victim's computer. The CERT/CC published information about the worm and advice on protecting systems in IN-2003-03.
- **MS-SQL Server Worm/W32.Slammer**
  Intruders used a piece of self-propagating malicious code referred to as the SQLSlammer, W32.Slammer, and Sapphire worm to exploit a vulnerability in the Resolution Service of Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000. The propagation of this malicious code caused varied levels of network degradation across the Internet and the compromise of vulnerable machines.

  The CERT/CC initially published CA-2002-22, describing several serious vulnerabilities in Microsoft SQL Server that allow attackers to obtain sensitive information, alter database contents, and compromise server hosts. When these and other vulnerabilities finally manifested themselves in the form of the MS-SQL Server Worm, the CERT/CC published advice in CA-2003-04.

Significant Vulnerabilities

Among the significant vulnerabilities this year are the two listed below.

- **Multiple Vulnerabilities in Microsoft RPC Interface**
  In CA-2003-16, the CERT/CC described multiple vulnerabilities in Microsoft's Remote Procedure Call (RPC) Interface that could allow an intruder to execute code or cause a denial of service. Two weeks after the advisory was published, the CERT/CC began receiving reports of

widespread scanning and exploitation of these vulnerabilities, leading to the publication of CA-2003-19.

- **Multiple Vulnerabilities in Internet Explorer**
  CA-2003-22 provides information about five vulnerabilities in Microsoft Internet Explorer. By exploiting these vulnerabilities, intruders could cause denial of service or execute code.

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

Advisories

The CERT/CC published 28 advisories in 2003. 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 list of advisories issued during 2003 can be found in Appendix A.

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 2003, we published 4 incident notes and 255 vulnerability notes.

Survivable Network Technology

Staff published numerous research papers in 2003 that deal with survivable network technology activities. The following samples are available on the CERT/CC web site:

- Technical Note: Requirements Engineering for Survivable Systems
- Special Report: International Liability Issues for Software Quality
- Paper: Trustworthy Refinement Through Intrusion-Aware Design (TRIAD): An Overview
- Technical Note: Applying FSQ Engineering Foundations to Automated Calculation of Program Behavior
- Technical Report: Trustworthy Refinement Through Intrusion-Aware Design (revision)

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. The archive includes 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 Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science, and Research and Development—"Cyber Security - Growing Risk from Growing Vulnerability"
- Testimony to the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census—"Viruses and Worms: What Can We Do About Them?"
- Testimony to the Library of Congress Copyright Office at the Rulemaking Hearing—Digital Millennium Copyright Act (DMCA)

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 *Software Design Magazine, Forbes Magazine, Vanity Fair, Wall Street Journal, Computerworld, Information*

Week, Network World, Chronicle of Higher Education, E-Commerce Times, Business 2.0, Boston Globe, Federal Computer Week, National Technology Review, Newsweek International Magazine, Information Security Magazine, IEEE Computer, CIO/CSO Magazine, Computer Magazine (Denmark), Wall Street Journal, eWeek, *Homeland Security & Defense Magazine, Washington Post, Toronto Star, Wired,* 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 National Public Radio, CBS News Radio, NBC, *60 Minutes*/CBS News, CNN, CNET, CMPTech Web, IDG News, ZDNet Australia, washingtonpost.com, and Internet-News.com.

The Blaster worm alone led to nearly 70 interviews with television, radio, and print news outlets, and the CERT/CC was mentioned or featured in more than 400 publications worldwide. Print outlets on this topic included the *New York Times*, the *Washington Post*, the *Wall Street Journal*, Dow Jones Newswires, and the Associated Press. Staff was interviewed on television by Tom Brokaw on the *NBC Nightly News*, MSNBC, the *Today Show*, and Lou Dobbs on CNN, among others. Radio interviews included those with WINS Radio All News in NYC and with WTOP in Washington, DC.

2.5. Training

The NSS Program offers nine training courses. Five courses derive from the work of the CERT/CC, providing introductory and advanced training for technical staff and the management of computer security incident response teams. Four courses are centered on 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 2003 included the following:

- *Concepts and Trends in Information Security*
- *Information Security for Technical Staff*
- *OCTAVE℠ Method Training Workshop*
- *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*
- *Information Survivability: A New Executive Perspective*

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.

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. In addition, we closely examine the activity reported by major archive sites and other computer security incident response teams.

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.

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/.

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 600 hardware and software developers.

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

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 2003:

- Forum of Incident Response and Security Teams (FIRST) Conference
- Internet Engineering Task Force (IETF) Meeting
- USENIX LISA 2003
- Network Security Information Exchange (NSIE)
- North American Network Operators Group (NANOG)
- Annual InfraGard Congress and Conference
- Asia Pacific Security Incident Response Coordination (ASPIRC) Conference
- IEEE International Requirements Engineering Conference
- ACM Conference on Computer and Communications Security
- Annual Computer Security Applications Conference
- Information Assurance Research and Development Symposium

3 Appendix A: CERT Advisories Published in 2003

The following advisories were published in 2003. We update the advisories as necessary. Advisories are available on the CERT web site at http://www.cert.org/advisories/.

CA-2003-01

Buffer Overflows in ISC DHCPD Minires Library

The Internet Software Consortium (ISC) has discovered several buffer overflow vulnerabilities in their implementation of DHCP (ISC DHCPD). These vulnerabilities may allow remote attackers to execute arbitrary code on affected systems. At this time, we are not aware of any exploits.

CA-2003-02

Double-Free Bug in CVS Server

A "double-free" vulnerability in the Concurrent Versions System (CVS) server could allow an unauthenticated, remote attacker with read-only access to execute arbitrary code, alter program operation, read sensitive information, or cause a denial of service.

CA-2003-03

Buffer Overflow in Windows Locator Service

A buffer overflow vulnerability in the Microsoft Windows Locator service could allow a remote attacker to execute arbitrary code or cause the Windows Locator service to fail. This service is enabled and running by default on Windows 2000 domain controllers and Windows NT 4.0 domain controllers.

CA-2003-04

MS-SQL Server Worm

The CERT/CC has received reports of self-propagating malicious code that exploits multiple vulnerabilities in the Resolution Service of Microsoft SQL Server 2000. The propagation of this worm has caused varied levels of network degradation across the Internet, in addition to the compromise of vulnerable machines.

CA-2003-05

Multiple Vulnerabilities in Oracle Servers

Multiple vulnerabilities exist in Oracle software that may lead to execution of arbitrary code; the ability to read, modify, or delete information stored in underlying Oracle databases; or denial of service. All of these vulnerabilities were discovered by Next Generation Security Software Ltd.

CA-2003-06

Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP)

Numerous vulnerabilities have been reported in multiple vendors' implementations of the Session Initiation Protocol. These vulnerabilities may allow an attacker to gain unauthorized privileged access, cause denial-of-service attacks, or cause unstable system behavior.

CA-2003-07

Remote Buffer Overflow in Sendmail

There is a vulnerability in sendmail that may allow remote attackers to gain the privileges of the sendmail daemon, typically root.

CA-2003-08

Increased Activity Targeting Windows Shares

In recent weeks, the CERT/CC has observed an increase in the number of reports of systems running Windows 2000 and XP compromised due to poorly protected file shares.

CA-2003-09

Buffer Overflow in Core Microsoft Windows DLL

A buffer overflow vulnerability exists in the Win32 API libraries shipped with all versions of Microsoft Windows 2000. This vulnerability, which is being actively exploited on WebDAV-enabled IIS 5.0 servers, will allow a remote attacker to execute arbitrary code on unpatched systems. Sites running Microsoft Windows 2000 should apply a patch or disable WebDAV services as soon as possible.

CA-2003-10

Integer overflow in Sun RPC XDR library routines

There is an integer overflow in the xdrmem_getbytes() function distributed as part of the Sun Microsystems XDR library. This overflow can cause 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-2003-11

Multiple Vulnerabilities in Lotus Notes and Domino

Multiple vulnerabilities have been reported to affect Lotus Notes clients and Domino servers. Multiple reporters, the close timing, and some ambiguity caused confusion about what releases are vulnerable. We are issuing this advisory to help clarify the details of the vulnerabilities, the versions affected, and the patches that resolve these issues.

CA-2003-12

Buffer Overflow in Sendmail

There is a vulnerability in sendmail that may allow remote attackers to gain the privileges of the sendmail daemon, typically root.

CA-2003-13

Multiple Vulnerabilities in Snort Preprocessors

There are two vulnerabilities in the Snort Intrusion Detection System, each in a separate preprocessor module. Both vulnerabilities allow remote attackers to execute arbitrary code with the privileges of the user running Snort, typically root.

CA-2003-14

Buffer Overflow in Microsoft Windows HTML Conversion Library

A buffer overflow vulnerability exists in a shared HTML conversion library included in Microsoft Windows. An attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service.

CA-2003-15

Cisco IOS Interface Blocked by IPv4 Packet

A vulnerability in many versions of Cisco IOS could allow an intruder to execute a denial-of-service attack against a vulnerable device.

CA-2003-16

Buffer Overflow in Microsoft RPC

A buffer overflow vulnerability exists in Microsoft's Remote Procedure Call (RPC) implementation. A remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service.

CA-2003-17

Exploit Available for the Cisco IOS Interface Blocked Vulnerabilities

An exploit has been posted publicly for the vulnerability described in VU#411332.

CA-2003-18

Integer Overflows in Microsoft Windows DirectX MIDI Library

A set of integer overflows exists in a DirectX library included in Microsoft Windows. An attacker could exploit this vulnerability to execute arbitrary code or to cause a denial of service.

CA-2003-19

Exploitation of Vulnerabilities in Microsoft RPC Interface

The CERT/CC is receiving reports of widespread scanning and exploitation of two recently discovered vulnerabilities in Microsoft Remote Procedure Call (RPC) Interface.

CA-2003-20

W32/Blaster worm

The CERT/CC is receiving reports of widespread activity related to a new piece of malicious code known as W32/Blaster. This worm appears to exploit known vulnerabilities in the Microsoft Remote Procedure Call (RPC) Interface.

CA-2003-21

GNU Project FTP Server Compromise

The CERT/CC has received a report that the system housing the primary FTP servers for the GNU software project was compromised.

CA-2003-22

Multiple Vulnerabilities in Microsoft Internet Explorer

Microsoft Internet Explorer (IE) contains multiple vulnerabilities, the most serious of which could allow a remote attacker to execute arbitrary code with the privileges of the user running IE.

CA-2003-23

RPCSS Vulnerabilities in Microsoft Windows

Microsoft has published a bulletin describing three vulnerabilities that affect numerous versions of Microsoft Windows. Two of these vulnerabilities are remotely exploitable buffer overflows that may allow an attacker to execute arbitrary code with system privileges. The third vulnerability may allow a remote attacker to cause a denial of service.

CA-2003-24

Buffer Management Vulnerability in OpenSSH

There is a remotely exploitable vulnerability in a general buffer management function in versions of OpenSSH prior to 3.7. This may allow a remote attacker to corrupt heap memory which could cause a denial-of-service condition. It may also be possible for an attacker to execute arbitrary code.

CA-2003-25

Buffer Overflow in Sendmail

A vulnerability in sendmail could allow a remote attacker to execute arbitrary code with the privileges of the sendmail daemon, typically root.

CA-2003-26

Multiple Vulnerabilities in SSL/TLS Implementations

There are multiple vulnerabilities in different implementations of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. These vulnerabilities occur primarily in Abstract Syntax Notation One (ASN.1) parsing code. The most serious vulnerabilities may allow a remote attacker to execute arbitrary code. The common impact is denial of service.

CA-2003-27

Multiple Vulnerabilities in Microsoft Windows and Exchange

There are multiple vulnerabilities in Microsoft Windows and Microsoft Exchange, the most serious of which could allow remote attackers to execute arbitrary code.

CA-2003-28

Buffer Overflow in Windows Workstation Service

A buffer overflow vulnerability exists in Microsoft's Windows Workstation Service (WKSSVC.DLL). A remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service.

Published April 5, 2004