Software Engineering Institute
Carnegie Mellon University

CERT® Coordination Center 1995 Annual Report

January 1996

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 was formed by the Advanced Research Projects Agency (ARPA) in November 1988 in response to the needs exhibited during an Internet security incident. Our charter is to work with the Internet community in detecting and resolving computer security incidents as well as taking steps to prevent future incidents. Our specific mission is to

- Provide a reliable, trusted, 24-hour, single point of contact for emergencies.
- Facilitate communication among experts working to solve security problems.
- Serve as a central point for identifying and correcting vulnerabilities in computer systems.
- Maintain close ties with research activities and conduct research to improve the security of existing systems.
- Initiate proactive measures to increase awareness and understanding of information security and computer security issues throughout the community of network users and service providers.

2 Activities and Services

2.1.1 Incident Response

From January through December 1995, the CERT Coordination Center received 32,084 email messages and 3,428 hotline calls. We handled 2,412 computer security incidents during this period. More than 12,000 sites were affected by these incidents, which involved 732 break-ins and nearly that many probes and pranks. Among the most serious intruder activities for 1995 are the following.

- IP spoofing. There was a surge in IP spoofing this year. The year began with an advisory about IP spoofing, and attacks continued throughout the year. In a matter of weeks during the summer, we received more than 170 reports of IP spoofing attacks or probes, many resulting in successful break-ins. We found that several sites believed incorrectly that they were blocking such packets, and other sites had planned to block them but hadn't yet done so.

- Network File Service (NFS) attacks. This year there was a large increase in the number of attacks relating to weaknesses in NFS. Many of the attacks were successful; moreover, programs to automate these attacks have become widespread in the intruder community. A successful attack usually results in the intruders gaining root access.

- Network scanning. Intruders have been scanning a large range of network addresses using Internet Security Scanner (ISS). This tool interrogates all computers within a specific address range, determining the security posture of each with respect to several common system vulnerabilities. Intruders have used the information gathered from these scans to compromise sites, and we are aware of many systems that have suffered a root compromise as a result of information intruders obtained from ISS scans.

- Packet sniffers. This year we continued to receive new incident reports about sniffers on compromised hosts. These sniffers, used to collect account names and passwords, frequently have been installed using a kit. In some cases, the packet sniffer was found to have been running for months. Occasionally, sites had been explicitly warned of the possibility of compromise, but the activity continued because the site did not address the problem in the comprehensive manner we suggest in our security documents.

- Sendmail attacks. Intruders have been using a variety of techniques to exploit sendmail, with most of the attacks aimed at getting root privileges on the victim machine. This year, we released four CERT advisories and one vendor-initiated bulletin relating to problems with sendmail. In many cases, intruder attacks were successful because sites had not installed upgrades and patches nor taken other precautions such as running the sendmail restricted shell program (smrsh).

The year ended with a series of attacks on Internet sites that resulted in our issuing an alert to network service providers and the network community in general warning them of the intruder activities listed below (list taken from advisory CA-95:18).

- Using automated tools to scan sites for NFS and NIS vulnerabilities
- Exploiting the rpc.ypupdated vulnerability to gain root access
- Exploiting the loadmodule vulnerability to gain root access
- Installing Trojan horse programs and packet sniffers
- Launching IP spoofing attacks

Work continues in 1996 on incidents involving all the types of activity noted in this annual report.

2.1.2 Advisories

Eighteen advisories were published in 1995. 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. Advisories are sent to the cert-advisory mailing list and posted to the USENET newsgroup comp.security.announce.

We use README files associated with each advisory to keep information current without changing the original content of an advisory.

A complete listing of the advisories issued during 1995 can be found in Appendix A.

2.1.3 Vendor Bulletins

In December 1994, we began publishing CERT vendor-initiated bulletins. These bulletins contain verbatim text from vendors describing security problems and their solutions. Our goal is to help the vendors' security information get wide distribution quickly. The bulletins are distributed through the same channels as advisories.

Ten bulletins were published in 1995. A complete listing can be found in Appendix B.

2.1.4 CERT Summaries

This year we began publishing the CERT Summary as part of our ongoing efforts to disseminate timely information about Internet security issues. The first CERT Summary was issued on July 26; others followed on September 26 and November 28. The primary purpose of the summary is to call attention to the types of attack currently being reported to the CERT incident handling staff. Each summary includes pointers to advisories or other publications that explain how to deal with the attacks.

2.1.5 Training Courses

CERT staff continued to present "Internet Security for System and Network Administrators" and "Internet Security for Managers." Both courses help organizations assess and improve their level of computer and information security.

This year, "Internet Security for System and Network Administrators" was approved by the SEI Education and Training Review Board as an SEI course. The course will be presented at the SEI four times during 1996: February 15, April 11, July 11, and December 11.

3 Research and Development

Information Security Risk Evaluations

During the year, we completed two field tests of an information security risk evaluation (ISRE) method being developed by the CERT staff. Both tests were conducted at financial service organizations. The ISRE includes a security taxonomy, a set of interviews, and a technology review.

The information security risk evaluation is one component of an overall information security improvement program under development. With the risk evaluation as a starting point, this program will provide practical guidance in addressing the issues and shortcomings that are identified as risk areas. The objective is to start a site on an improvement path in a way that ensures a high probability of success.

4 Advocacy and Community Support

The CERT Coordination Center staff members were invited to give presentations at several conferences, workshops, and meetings during 1995. This has been found to be an excellent tool to educate attendees in the area of network information system security and incident response. Below are some examples of the CERT staff's participation in external events.

- Avoiding the Crisis in Healthcare Information Security, a conference sponsored by MIS Training and INFO Security. A CERT staff member presented "Securing your Interface to the Internet."
- FBI Academy. A CERT staff member spoke on Internet security issues and the use of the Internet.
- Institute of Internal Auditors (IAA). At the IAA Advanced Technology Conference held September 16-20, 1995, a staff member gave a talk on "Defensive Strategies on the Information Highway."
- Internet Symposium on Network and Distributed System Security. A CERT staff member served as the general chair of the three-day symposium.
- NISSC (National Information Systems Security Conference - formerly National Computer Security Conference). A CERT member presented "Internet Sniffer Attacks," which won outstanding paper for the conference.
- Public meeting on National Information Infrastructure (NII) Security Issues. A CERT team member testified at a public meeting held at the Department of Commerce in March. Topics included the risks to information, educating and setting expectations of users, and how the government can support availability and reliability in the NII.
- SEC EDGAR Technology Conference. A staff member participated in a panel entitled "Technical Options for Achieving Fundamental Objectives."
- Uniforum UNIX show. A CERT staff member presented an all-day tutorial, "Internet Security for UNIX System and Network Administrators," to 82 people. He also presented "Managing the Risk" to more than 50 people during a regular session of the conference.
- The USENIX Association presented team member Jim Ellis with the USENIX Lifetime Achievement Award. This award recognizes and celebrates singular contributions to the UNIX community in both intellectual achievement and service that are not recognized in any other forum. For 1995, Ellis and two others received the award for their work in creating USENET.

4.1 Internet Engineering Task Force

The CERT Coordination Center is actively involved in the security-related work of the Internet Engineering Task Force (IETF). CERT staff member Barbara Fraser is a member of the Security

Directorate, a standards body, and is chair of two workings groups. The working groups are producing two site security handbooks - one for system and network administrators, and one for users - and are developing guidelines for security incident response teams and technology vendors.

4.2 Forum of Incident Response and Security Teams

The CERT Coordination Center co-sponsored the FIRST Incident Response Workshop, which was held in Karlsruhe, Germany, September 18-22, 1995. There were 129 attendees, representing more than 30 response teams from around the world. This annual workshop provides a forum for teams to exchange information and discuss ways to coordinate response activities. Topics this year included how to form an incident response team, communication among teams, recent developments in network liability, and techniques for tracking incidents.

Appendix A: CERT Advisories Published in 1995

The following advisories were published in 1995. We will continue to add updated information to CA-95:xx.README files as necessary.

CA-95:01.IP.spoofing.attacks.and.hijacked.terminal.connections
This advisory describes attacks in which intruders create packets with spoofed IP addresses and exploit applications that use authentication based on IP. The advisory also discusses a tool intruders use to take control of open terminal or login sessions.

CA-95:02.binmail.vulnerabilities
This advisory supersedes CA-91:01a and CA-91:13. It addresses vulnerabilities in some versions of /bin/mail based on BSD 4.3 UNIX. It includes a list of vendor patches and source code for mail.local.c, an alternative to /bin/mail. Updated information will be placed in the CA-95:02.README file.

CA-95:03.telnet.encryption.vulnerability
Description and patch information for a security problem in the Berkeley Telnet clients that support encryption and Kerberos V4 authentication. **This information is superseded by CA-95:03a.

CA-95:03a.telnet.encryption.vulnerability
Description and patch information for a security problem in the Berkeley Telnet clients that support encryption and Kerberos V4 authentication. It provides additional information. **This information supersedes CA-95:03.

CA-95:04.NCSA.http.daemon.for.unix.vulnerability
This advisory provides a patch for a vulnerability in the NCSA HTTP daemon version 1.3 for UNIX.

CA-95:05.sendmail.vulnerabilities
This advisory supersedes all previous advisories relating to sendmail. Three vulnerabilities are addressed; vendor vulnerability and patch information is included, along with a sendmail wrapper.

CA-95:06.satan
An overview of the Security Administrator Tool for Analyzing Networks (SATAN) based on the CERT staff's review of beta version 0.51. Includes a list of vulnerabilities probed and advice on securing systems.

CA-95:07.vulnerability.in.satan
This advisory describes precautions to take against a vulnerability in SATAN 1.0. **Superseded by CA-95:07a.

CA-95:07a.REVISED.satan.vul
This revised advisory supersedes CA-95:07. The revision provides new information about the problem described in CA-95:07, and includes precautions to take when running SATAN. A tutorial by the SATAN authors, "SATAN Password Disclosure," is appended to the advisory.

CA-95:08.sendmail.v.5.vulnerability
This advisory describes a vulnerability in sendmail v.5, which is still in use and which includes IDA sendmail. Many vendors have previously fixed the problem; others recently developed patches.

CA-95:09.Solaris.ps.vul
This advisory describes a vulnerability in Solaris that can be exploited if the permissions on the /tmp and /var/tmp directories are set incorrectly.

CA-95:10.ghostscript
This advisory describes a vulnerability involving the -dSAFER option in ghostscript versions 2.6 through 3.22 beta. The advisory includes instructions for fixing the problem and pointers to version 3.33 of ghostscript.

CA-95:11.sun.sendmail-oR.vul
This advisory describes a vulnerability in the sendmail -oR option in SunOS 4.1.X. At the time of the advisory, the vulnerability was being actively exploited.

CA-95:12.sun.loadmodule.vul
The advisory describes a problem with the loadmodule(8) program in Sun OS 4.1.X and provides patch information.

CA-95:13.syslog.vul
This advisory describes a general problem with syslog, lists vendor information about patches, and provides a workaround for solving the syslog problem in sendmail in particular.

CA-95:14.Telnetd_Environment_Vulnerability
This advisory describes a vulnerability with some telnet daemons and includes patch information from vendors, along with a workaround.

CA-95:15.SGI.lp.vul
This advisory points out accounts that are distributed without passwords and urges SGI customers to create passwords for those accounts.

CA-95:16.wu-ftpd.vul
This advisory describes a vulnerability in the wu-fptd SITE EXEC command and provides solutions for both Linux users and others.

CA-95:17.rpc.ypupdated.vul
This advisory describes a vulnerability in the rpc.ypupdated program, for which an exploitation program has been posted to several newsgroups. The advisory includes vendor information and a workaround.

CA-95:18.widespread.attacks
This advisory warns readers of attacks on hundreds of Internet sites in which intruders exploit known vulnerabilities, all of which have been addressed in previous CERT advisories. These advisories are listed.

Appendix B: CERT Vendor-Initiated Bulletins Issued in 1995

The following vendor-initiated bulletins were published in 1995.

VB-95:01.hp
This bulletin addresses problems with Remote Watch in fileset WATCH-RUN for releases of HP-UX, in particular HP 9000 series 300/400s 10.2(1) through 10.2(5); 10.0(1) through 10.0(9); and all previous versions.

VB-95:02.sgi
Vulnerability and patch information for the IRIX 5.2, 6.0, 6.0.1 Desktop Permissions Tool.

VB-95:03.hp
Sendmail vulnerability and patch information for HP 9000 series 300/400s and 700/800s 8.x and 9.x.

VB-95:04.venema
Vulnerability and patch information for S/Key software enhancements for FreeBSD 1.1.5.1 and 2.0 and for logdaemon versions prior to 4.9.

VB-95:05.osf
Description of a security hole in all releases of OSF/DCE prior to version 1.1, and information about the fix.

VB-95:06.cisco
Problem description, upgrade information, and workaround for a vulnerability in Cisco's IOS software versions 10.3(1) through 10.3(2); 10.2(1) through 10.2(5); 10.0(1) through 10.0(9); and all previous versions.

VB-95:07.abell
Description of a directory and file vulnerability in lsof 3.18 through 3.43, along with instructions on getting later versions.

VB-95:08.X_Authentication_Vul
Vulnerability and patch information for an X authentication vulnerability.

VB-95:09.hp
Vulnerability and patch information for a vulnerability in ftp in releases 9.X and 10.X of HP-UX (platforms: HP 9000 series 300/400s and 700/800s).

VB-95:10.elm
Vulnerability and patch information for a vulnerability in elm 2.4 PL 24.

VB-95:10a.elm
This updated version of VB-95:10 lists additional FTP sites.